NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IMPLEMENTATION OF A MODULAR FLY AWAY KITS (FLAK) FOR C4ISR IN ORDER TO COUNTER ASYMMETRIC THREATS IN THE COALITION RIVERINE AND MARITIME THEATRES

by

Robert Hochstedler

June 2006

Thesis Advisor: James F. Ehlert
Second Reader: Rex Buddenberg

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Implementation of a Modular Fly away Kits (FLAK) for C4ISR in order to counter Asymmetric Threats in the Coalition Riverine and Maritime Theatres**.**		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Robert Hochstedler			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

This research analyzes the design and implementation of a Maritime Command, Control, Computer, and Communications for Intelligence, Surveillance, and Reconnaissance (C4ISR) fly away kit (FLAK) in order to combat asymmetric threats in the coalition maritime environment. This FLAK will be modular, adaptable, scalable, and secure end to end, composed of routable networks, and built entirely from commercial off the shelf technologies (COTS). Basing measures of effectiveness (MOE) on the recently published Quadrennial Defense Report (QDR) and the Numbered Fleet Commanders Communication Message, these kits will be tested with the goal of fulfilling thirteen of the fifteen high priority short-falls in the modern United States CIV-MIL and Coalition Forces' abilities to conduct multiple missions in the current brown (riverine), green (littoral), and blue (deep water) operational theatres.

The Maritime FLAK will be designed with the intent of increasing the US forward presence and extending the C4ISR into restricted maritime theatres. Since US forces cannot intervene directly into regions like the Straits of Malacca, but can support coalition forces through advisors and technological adaptations, modular solutions to extend C4ISR into these maritime territories are needed. Furthermore, due to the adaptability and scalability of the technologies to be implemented into the maritime FLAK, these completed kits will be able to be used by the recently formed Naval Expeditionary Combat Command (NECC) in current operations in the Global War on Terrorism.

14. SUBJECT TERMS IEEE 802.16 , Wireless, Maritime Security, Riverine, NECC, GWOT, 802.11, VBSS Integrated Sensors, TCP/IP, MANET, FLAK, Radio-WAN			**15. NUMBER OF PAGES** 145
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

IMPLEMENTATION OF A MODULAR FLY AWAY KITS (FLAK) FOR C4ISR IN ORDER TO COUNTER ASYMMETRIC THREATS IN THE COALITION RIVERINE AND MARITIME THEATRES

Robert A. Hochstedler
Lieutenant, United States Navy
B.A., Dickinson College, 1995

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY
(COMMAND, CONTROL AND COMMUNICATIONS (C3))**

from the

**NAVAL POSTGRADUATE SCHOOL
June 2006**

Author: Robert Hochstedler

Approved by: James F. Ehlert
Thesis Advisor

Rex Buddenberg
Second Reader

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research analyzes the design and implementation of a Maritime Command, Control, Computer, and Communications for Intelligence, Surveillance, and Reconnaissance (C4ISR) fly away kit (FLAK) in order to combat asymmetric threats in the coalition maritime environment. This FLAK will be modular, adaptable, scalable, secure end-to-end, composed of routable networks, and built entirely from commercial off the shelf technologies (COTS). Basing measures of effectiveness (MOE) on the recently published Quadrennial Defense Report (QDR) and the Numbered Fleet Commanders Communication Message, these kits will be tested with the goal of fulfilling thirteen of the fifteen high priority short-falls in the modern United States CIV-MIL and Coalition Forces' abilities to conduct multiple missions in the current brown (riverine), green (littoral), and blue (deep water) operational theatres.

The Maritime FLAK will be designed with the intent of increasing the US forward presence and extending the C4ISR into restricted maritime theatres. Since US forces cannot intervene directly into regions like the Straits of Malacca, but can support coalition forces through advisors and technological adaptations, modular solutions to extend C4ISR into these maritime territories are needed. Furthermore, due to the adaptability and scalability of the technologies to be implemented into the maritime FLAK, these completed kits will be able to be used by the recently formed Naval Expeditionary Combat Command (NECC) in current operations in the Global War on Terrorism.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. BACKGROUND....1
B. OBJECTIVES....4
C. RESEARCH QUESTION....5
D. SECONDARY QUESTIONS....5
E. SCOPE....6
F. CHAPTER BY CHAPTER SUMMARY....6

II. MODERN RIVERINE WARFARE / MARITIME SECURITY....9
A. MARITIME SECURITY....9
1. Maritime Environment....9
2. Maritime Security Strategic Initiatives....13
3. National Fleet Concept....17
4. International Maritime Security Initiatives....18
5. Coalition Security Initiatives....20
B. RIVERINE WARFARE....24
1. History of Riverine Warfare....24
2. Current Riverine Environment....28
3. Modern Riverine Doctrine....28
C. NAVAL EXPEDITIONARY COMBAT COMMAND (NECC)....30
D. MARITIME AND RIVERINE CRAFTS....31
1. Rigid Hull Inflatable Boats (RHIB)....32
2. Special Operations Craft – Riverine (SOC-R)....33
3. Small Unit Riverine Craft (SURC)....34
4. Special Operations Craft – MK V PEGASUS....36
5. USCG Harbor Security and Motor Life-Boats (Mlb)....37
6. Coalition Forces....38
7. Junk Force Craft....39
E. SUMMARY....39

III. MOBILE AD-HOC NETWORKING....41
A. NETWORK-CENTRIC WARFARE (NCW)....41
1. The Global Information Grid....42
2. Usn/Usmc – FORCEnet....44
3. USCG – Deepwater....47
4. DIGITAL DIVIDE....47
B. MOBILE AD-HOC NETWORKING (MANET)....49
C. IEEE 802.16....52
1. IEEE 802.16 Background....52
2. Military Applications of IEEE 802.16....54
3. IEEE 802.16e....55
D MARITIME NETWORK TOPOLOGIES FOR IEEE 802.16 ARCHITECTURES....57

1. VBSS Topology 57
2. Riverine – Craft to Craft & Craft to Shore (Vehicle or Choke Point Security) 58
3. Harbor & Port Security 59

IV. MARITIME FLY AWAY KIT TECHNOLOGY 61
A. M-FLAK TOPOLOGY 61
1. Network Components 63
a. Redline AN-50e Communications Bridge 63
b. Redline AN-50M Communications Bridge 63
c. Hyperlink Sectored 360 degree Omni-array 64
d. D-Link Commercial Ethernet Switch 66
e. AKCP Sensor Probe Eight Linux (SP8L) 67
2. M- FLAK End Systems 69
a. Kestrel-Tech wearable USB Camera 69
b. Modular Computing Company's (MCC) Modular PC 70
3. Miscellaneous M-FLAK Equipment 72
a. SKB Roll-Shock Case 72
b. Power 73
4. Miscellaneous Network Equipment 74
a. C3Trak Shared Situational Application (SSA) 74
b. 802.11g Mesh Dynamics Access Point 75
c. Identix Biometrics Handheld Unit 76
d. Air Force Battle Lab (AFBL) Explosive Material Device 76
e. CISCO Tactical Communications Kit (TCK) 77
B. COMBINED M-FLAK 79
1. Small Boat 79
2. Boarding Officer 79

V. LABORATORY AND FIELD EXPERIMENTATION 81
A. COALITION OPERATING AREA SURVEILLANCE AND TARGETING SYSTEM (COASTS) EXPERIMENTS 81
1. Background 81
2. Network Architecture 82
3. Measures of Performance (MOP) 87
4. Measure of Effectiveness (MOE) 88
5. Pre-Deployment Exercises (December 2006) 89
6. Pre-Deployment Exercises (February 2006) 92
7. COASTS Deployment to Thailand (March 2006) 96
8. Monterey USCG Maritime Tests (April 2006) 100
9. COASTS Deployment to Thailand (May 2006) 102

VI. CONCLUSION 107
A. RESEARCH SUMMARY 107
B. LESSONS LEARNED 110
1. Overall Network Lessons Learned 111
a. IEEE 802.16 Antenna Placement 111

b. AN-50e and AN-50M Terminals 111
2. End Systems Technologies 111
a. Kestrel Camera 111
b. Patrolcam 112
c. Identix IBIS 112
d. Modular PC 113
C. FUTURE RESEARCH AREAS AND QUESTIONS 113
1. Critical Research Areas 113
a. Electronic Steerable Antennas (ESA) 113
b. IEEE 802.16 Amplifiers 114
c. Norsat 5200 KU-10W-P3K 114
d. Riverine Maritime Security Coalition Communications Doctrine 115
e. Alternate COTS IEEE 802.16 Commercial Vendors 115
f. Multi-boat PtMP IEEE 802.16 Testing 116
g. Alternate Network Topologies 116
2. Secondary Research Areas 116
a. Riverine M-FLAK CONOPS 116
b. Extended M-FLAK Periphery Technologies 117
c. Design of a USCG Coastal Maritime Radio-WAN 117
3. Tertiary Research Areas 117
a. Integration into the Hastily Formed Network (HFN) Humanitarian Assistance/Direct Response (HA/DR) 117
b. Life-cycle Management Costs of Operating a Squadron of Small Boats with the M-FLAK 118
D. SUMMARY 118
LIST OF REFERENCES 119
INITIAL DISTRIBUTION LIST 123

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Damage to the USS COLE (DDG 67) after the October 2000 terrorist assault....10
Figure 2. 2005 Pirate Attacks in the KAA....12
Figure 3. Damage to the French Tanker Limburg after a terrorist assault....13
Figure 4. Insignia for the recently formed Malaysian Maritime Enforcement Agency..23
Figure 5. Naval Special Warfare RHIB....33
Figure 6. Naval Special Operations Craft – Riverine (SOC-R)....34
Figure 7. USMC Small Unit Riverine Craft (SURC)....35
Figure 8. Special Operations Warfare Craft MK V Pegasus....36
Figure 9. USCG Harbor Security Patrol Boats....37
Figure 10. USCG Motor Life Boats (MLB)....37
Figure 11. Indonesian Frigate patrolling the Straits of Malacca....38
Figure 12. Network-Centric Warfare diagram of the Global Information Grid (GIG)....43
Figure 13. FORCEnet 21 as an integrated composite of Sea Power 21....45
Figure 14. Deepwater Assets to be integrated into the full NCW architecture....47
Figure 15. MANET Architecture versus the OSI model architecture....50
Figure 16. Information System Principle #1....51
Figure 17. Information System Principle #2....52
Figure 18. VBSS Network Topology for the M-FLAK....58
Figure 19. Riverine M-FLAK Topology....59
Figure 20. Harbor Security Topology....60
Figure 21. M-FLAK component technology – IS Principle #1 Architecture....61
Figure 22. M-FLAK Network Topology – Information System #2 Architecture....62
Figure 23. AN-50e Wireless Base Station....63
Figure 24. AN-50M Wireless Base Station....64
Figure 25. Hypergain HG5817P-090 Wifi antenna array....64
Figure 26. RF Propagation form the Sectored Omni Array....65
Figure 27. RF Propagation from the Sectored antenna....65
Figure 28. Superpass 13 dbi antenna....66
Figure 29. D-link four-port Ethernet Switch....67
Figure 30. AKCP SP8L Box – Front View....68
Figure 31. AKCP SP8L Box – Back View....68
Figure 32. Kestrel-Tech USB Powered Camera worn by LT Hochstedler in Thailand....70
Figure 33. Modular PC....71
Figure 34. Patrolcam and Proprietary joystick....72
Figure 35. SKB Roll Shock Case 6R....73
Figure 36. UB2590 And 12 volt batteries....73
Figure 37. Shared Situation Awareness (SSA) applications C3 Track....75
Figure 38. IEEE 802.11g Mesh Dynamics Wireless Access Point (AP)....75
Figure 39. Identix Biometrics Reader....76
Figure 40. AFBL Explosive Materials Detection Device....77
Figure 41. Tactical Communications Kit (TCK)....78

Figure 42. M-FLAK on the Speedboat during the May 2006 COASTS deployment.....79
Figure 43. LT Hochstedler in the Boarding Officer gear using Kestrel Camera and Wearable Modular PC.....80
Figure 44. COASTS 2006 Logo.....81
Figure 45. COASTS Mae Ngat Dam Operating Area (AO).....83
Figure 46. COASTS 2006 Global Network Topology.....85
Figure 47. Overall Mae Ngat Dam Network Topology.....86
Figure 48. COASTS 2006 Maritime Network Topology.....87
Figure 49. USN SOSUS Station Pt Sur, CA Sonar Station.....89
Figure 50. 90 Degree 5.8 GHz antenna w/ T-58 Transceiver.....93
Figure 51. Tactical Operating Center.....97
Figure 52. 180 degree array used at the Mae Ngat Dam during testing.....98
Figure 53. 360 degree omni-sector array using 13 dBi 90 degree sectored antennas.....98
Figure 54. SKB Case with the Modular PC mount.....99
Figure 55. Shore Array used during PtMP testing at the USCG pier in Monterey, CA .101
Figure 56. LT Hochstedler operating M-FLAK on Thailand longboat.....105

LIST OF TABLES

Table 1. Point Sur PtMP IX Chariot throughput tests (straightaway driving).....90
Table 2. PT Sur Erratic Driving IX Chariot results 91
Table 3. Point Sur Erratic Driving IX Chariot results - reduced throughput due to vehicle superstructure 91
Table 4. FHL Throughput tests.....94
Table 5. FHL Throughput tests.....95
Table 6. FHL Throughput tests during JIOC Jamming 96
Table 7. RF distance test to 3NM in the Monterey Bay 102
Table 8. RF Monitor Results from a high speed run (23 Knots) on the Mae Ngat Dam.....104

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I have many people to thank for their aid in the completion of this thesis. First and foremost, the entire COASTS 2005 and 2006 teams. Their help empowered me to achieve more than I ever thought possible during my time here at Monterey.

Special thanks are required for Ryan Hale and Jonathon Powers, who troubleshot and argued concepts with me every step of the way as well as bought the drinks when they were needed. GO A-TEAM! And thanks to every reservist, COASTS team member and classmate during my time at NPS. They all helped in more ways than can be counted.

Thanks to Dr. Shoup who saw my work as worth funding. Thanks to the SPAWAR Fellowship review board, who for two years told me my work was "technologically unfeasible," giving me the proper motivation to prove them wrong.

Thanks to Rex Buddenberg who always calmed my scholastic stresses with an old fashioned Coast Guard sea story. Thanks to LCOL Karl Pfieffer, USAF who was the first in the fight whenever I needed help. Thanks to Jim Ehlert, who not only believed in my work, but made me an equal partner in achieving what had never been done before.

Finally, thanks to my wife for all she has done for me to enable me to complete this thesis. She is the only person who could make this much effort worthwhile.

ACRONYMS AND ABBREVIATIONS

AIS	Automated Identification System
BS	Base Station
C4ISR	Command, Control, Computers, and Communications for Intelligence, Surveillance, and Reconnaissance
CHD	Complex Humanitarian Disasters
COASTS	Coalition Operating Area Surveillance and Targeting System
COP	Common Operating Picture
DO	Distributed Operations
DoD	Department of Defense
DRDO	Defense Research Development Organization
DSL	Digital Subscriber lines
EPLRS	Enhanced Position Location Systems
ESA	Electronic Steer-able Antenna
FHL	Fort Hunter-Ligget
GMII	Global Maritime Intelligence Initiative
GPS	Global Positioning System
GWOT	Global War on Terrorism
HFN	Hastily Formed Networks
IDS	Integrated Deepwater System
IEEE	Institute of Electrical and Electronics Engineers
IIFC	Inter-agency Intelligence and Fusion center
IMO	International Maritime Organization
ISPS	International Ship and Port Facility Code
ISR	Intelligence, surveillance, and reconnaissance
JFMCC	Joint Force Maritime Component Command
JIATF-W	Joint Interagency Task Force West
JUSMAGTHAI	Joint United States Military Advisory Group Thailand
KAA	Khwar Abd Allah
LAN	Local area Network
LFA	Lead Federal Agency

LOS	Line of sight
MAC	Media Access Layer
MALSINDO	Malaysia Singapore Indonesia
MDA	Maritime Domain Awareness
MCK	Mobile Communications Kit
MIO	Maritime Interdiction Operations
MMEA	Malaysian Maritime Enforcement Agency
NCW	Network-centric warfare
NECC	Naval Expeditionary Combat Command
NGO	Non-governmental Organizations
NKGM	Knowledge Management
NLOS	Non-line of Sight
NMIC	National Maritime Intelligence Center
NORM	Nak-only reliable multicast
NPS	Naval Postgraduate School
OEF	Operation Enduring Freedom
OFDM	Orthogonal Frequency Division Multiplexing
OIF	Operation Iraqi Freedom
OSPF	Open Shortest Path First
OTM	On the move
PHY	Physical Layer
PSI	Proliferation Security Initiative
PtMP	Point to Multi-point
QDR	Quadrennial Defense Report
QoS	Quality of Service
RMSI	Regional Maritime Security Initiative
RTARF	Royal Thai Air Force
RV	Recreational Vehicle
SINGARS	Single Channel Air-Ground Radios Systems
SNMP	Simple Network Management Protocol
SOLAS	Safety of Life at Sea
STOM	Ship to objective maneuver

TCP	Transmission Control Protocol
TNT	Tactical Network Topology
US	United States
USCG	United States Coast Guard
USN	United States Navy
USMC	United States Marine Corps
USSR	Union of Soviet Socialists Republic
USPACOM	United States Pacific Command
USSOCOM	United States Special Operations Command
WAN	Wide area network
WCO	World Customs Organization
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
XML	Extensible Mark-up Language

I. INTRODUCTION

A. BACKGROUND

The maritime theatre has changed significantly in the post-Cold War world. In place of massed conventional navies patrolling the oceans, new asymmetric threats have risen to threaten the world's waterways. The commencement of the Global War on Terrorism (GWOT) only accelerated the need to address these threats. As stated by retired Coast Guard Officer Bruce Stubbs in a recent Heritage Foundation article:

> The likelihood of major combat operations at sea has diminished for the next two to three decades. In its place, maritime security against numerous non-military, non-traditional, asymmetric threats – terrorists, criminals, pirates, smugglers, and assorted miscreants – are highly likely. These threats must be defeated, preferably at their origin, or well before they reach America's shores. This new national security environment places much greater emphasis on maritime security or constabulatory operations for the purpose of "good order and discipline" at sea[1].

In order to counter these threats in the maritime theatre, the United States Navy (USN) must not only enhance its security on its blue water forces, but expand its role in the littoral (green water) and riverine (brown water) theatres.

To accomplish this, US forces must be able to patrol the vast reaches of the maritime theatre with a continually shrinking number of vessels, regardless of their distance from American Shores[2]. "Unsecured or ungoverned seas are potential havens for criminal or terrorist activity, providing relatively cheap and inconspicuous movement. And the thousands of miles of coastline many of us enjoy, are sometimes uninhabited and often difficult to regulate[3]. To counter these threats, the USN has expanded its GWOT mission requirements.

The current expansion of mission requirements for the USN in the GWOT includes:

---

[1] Stubbs, p. 1

[2] Footnote concerning the reduction in ship numbers from the planned Cold War levels of the 600 ship Navy – current levels equal 281 vessels.

[3] Definition of the Regional Maritime Security Initiative (RMSI) from www.globalsecurity.org

- Maritime Intercept Operations (MIO) aimed at identifying and intercepting terrorists or weapons of mass destruction at sea, or potentially threatening ships or aircraft approaching U.S. territorial waters – an activity that includes Navy participation in the multilateral Proliferation Security Initiative (PSI)
- Working with the Coast Guard to build and maintain maritime domain awareness (MDA) – a real-time understanding of activities on the world's oceans
- Assisting the Coast Guard in port-security operations
- Protection of forward-deployed Navy ships
- Protection of Navy Bases and facilities in the United States and elsewhere
- Development of a Riverine Warfare capability[4]

To summarize the Navy's GWOT roles as mandated by the US congress, the US Naval fleet must not only expand its presence in remote regions far from continental US soil, it must also integrate further with the United States Coast Guard (USCG) to develop a National Fleet which can create a layered and interchangeable defense in depth to counter all levels of maritime threats, both conventional and unconventional.

Even if the goal of an integrated and interoperable "National Fleet" is accomplished, there will be insufficient forces to patrol all of the globe's waterways. This places a heavy demand on the USN/USCG National Fleet's ability to increase its layered defense through the enhancement of the US' security relationships with allies overseas. To counter these non-traditional threats far away from the borders of the United States (US), the National Fleet must extend its C4ISR into maritime territories it has been previously unable to reach[5].

Therefore, in order to accomplish this mission, the US does not need to add newer platforms or weapons systems, but instead to improve its command and control interoperability not only within the newly designated National Fleet, but also with coalition Naval and Coast Guard Forces around the globe. The guiding principle of homeland security sums this situation up very well in the sixth principle – an unprecedented level of information sharing is required by all agencies[6].

4 According to a recent CRS report to Congress on the role of the Navy in the GWOT – Ronald O' Rourke

5 Malaysia and Indonesia rejected the US Pacific Commander ADM Fargo's request to have 7th Fleet USN/USMC forces patrol the Straits of Malacca as a deterrent to maritime piracy and terrorism - 2004

6 USCG MSHLS Introduction

The difficulty of integrating the communications of more than one military service has been a challenge faced by military forces for some time. With the addition of law enforcement forces, various government agencies, and humanitarian response groups, this problem increases in unprecedented complexity. Once the issue of coalition military forces is added into the question, this becomes a "Gordian Knot" of problem-solving[7]. This is especially true today, when current naval communications are inadequate to maintain the modern national fleet with its overwhelming GWOT mission requirements.

In a recent communications message from the Numbered Fleet Commanders in the US Navy, ten priorities were listed, focusing on the state of current communications in the USN. These ten priorities are:

1. Coalition Communications
2. Reliable SATCOM
3. Communications Standards
4. Lack of Adequate Data Throughput
5. Computer Network Defense (CND)
6. Common Operating Picture (COP)
7. Real-time Collaboration
8. Streamline processes to support emergent operational requirements
9. Next generation knowledge management (NGKM)
10. Incorporate Wireless Technology[8]

All of these priorities describe shortfalls within the current Command, Control, Computer, and Communications for Intelligence, Surveillance, and Reconnaissance (C4ISR) capabilities of the US forces. Based on ever-growing mission requirements of Joint US Forces, these current shortfalls must be compensated for; especially since the increase of new force dynamics to counter these threats will increase the requirements on the already disadvantaged users completing these missions.

[7] Gordian Knot refers to the myth of Alexander the Great's slice of the knot created by the Gordian kings, which was rumored to be impossible to be untied. It is used to refer to impossibly complex problems.

[8] Numbered Fleet Communications Requirements Message

The small boat operators[9], who will become the centerpiece of both riverine and maritime security operations, are also focused on in the Numbered Fleet Communications message. As stated in the message:

> Operational examples include the use of wireless communication from small boat operators to parent platforms in support of Electronic Maritime Interdiction Operations (EMIO). In this case, critical data collected by the Boarding party was quickly transmitted to the supporting intelligence element, thereby significantly reducing boarding time.
>
> The Navy must continue to support and develop its ISRT capabilities, systems, and processes to operate in a joint environment, especially in asymmetric operations in the GWOT. An over the horizon ISR transmission and reception system needs to be fielded to allow ships to stand off hostile coasts while ISR assets are able to penetrate to collection areas[10].

In other words, these capabilities must be linked to - and integrated with - a user historically removed from traditional naval C4ISR architectures. To achieve success in the future of maritime operations in the GWOT, these disadvantaged "last mile" operators must become fully linked into modern network-centric warfare (NCW) architectures.

B. OBJECTIVES

This research addresses the necessity of using a versatile and modular C4ISR Radio-WAN network architecture to maintain communications in the riverine and maritime theaters. The maritime theatre includes blue, green, and brown water environments.

The disadvantaged user in the maritime environment is the small boat operator. Due to the numerous missions they are required to accomplish without the network

[9] Small boats, which are the primary operators in maritime security, maritime interdiction operations (MIO), and riverine operations, do not have the multiple communications capabilities which have been developing along the Network Centric Warfare (NCW) transformation in larger vessels. Much like the individual foot soldier, logistics and power considerations have historically prevented the link of communications to these operators. The technological revolution is changing this link to the "disadvantaged user." It is important to note that, unlike the foot solider, the small boat has electrical power, like the HUMVEE and tank, and therefore can be empowered as a communications rely more easily than a foot soldier. This enables more connectivity to the small boat operator, who like the foot soldier, relies on battery power for communications links.

[10] Ibid

connectivity of the larger ships, they are more separated from NCW development than any other vessel. Increasing speed of data collection and linking the most remote operator to the collective intelligence databases around the world will greatly increase the power to counter asymmetric threats in the maritime environment.

The connectivity of C4ISR systems to the operators across the digital divide must be established not only to empower the distributed operator, but to increase the speed of digital reach-back to the remote commander and intelligence collector.

C. RESEARCH QUESTION

Can IEEE 802.16 Point to Multi-point (PtMP) wireless networking technologies be adapted for command, control, communications, computers for intelligence, surveillance, and reconnaissance (C4ISR) to be utilized by coalition maritime security forces in the defense against asymmetric threats in riverine, littoral, and other maritime theatres?

D. SECONDARY QUESTIONS

- Does IEEE 802.16 PtMP support tactical coalition operations in the maritime security theatre?
- Does IEEE 802.16 PtMP have applicability to be an effective C3I application?
- What IEEE 802.16 PtMP topology considerations should be considered?
- How does the IEEE 802.16 PtMP technology affect Naval Coastal Warfare Detachment and Special Boat Unit tactical doctrines?
- Can connectivity be maintained in maritime interdiction operations using the maritime FLAK?
- Can the FLAK be produced using Commercial-off-the-Shelf equipment (COTS) in a cost-effective manner?
- Can the maritime FLAK be integrated into the Global Information Grid (GIG)?

E. SCOPE

The Scope of this thesis will include:

1. An analysis of current force transformation being pursued by the US Department of Defense (DoD) and the Department of Homeland Security (DHLS). This review will focus primarily on current USN and USCG mission requirements, and the assets being used to accomplish those mission goals in the coalition maritime security environment. This includes shore-based port facilities as well as ships at sea.

2. An analysis of current IEEE 802.16 technologies under the kinematics test parameters involving high-speed mobility. The focus of this will be to hypothesize the potential of IEEE 802.16 technologies to the high-speed mobile user.

3. Finally, the test configurations will be conducted with tests for bandwidth, RF propagation, scalability, and functionality in a defined collaborative scenario test with other technology and coalition military tactical operators.

4.

F. CHAPTER BY CHAPTER SUMMARY

CHAPTER I

Introduction: This chapter highlights the obstacles facing the USN and its coalition allies in the current maritime theatre, including riverine and littoral environs. Current force transformation, increased mission requirements, and communications requirements to fulfill those missions will be introduced in this first chapter.

CHAPTER II

Maritime Security and Riverine Warfare: This chapter will focus on the modern maritime domain and the operations required of coalition forces in that environment. A study of the National Security Strategy (NSS), National Maritime Security Strategy (MHLS), and the recently published Quadrennial Defense Report (QDR) will be used to further highlight the requirements of the modern coalition maritime forces. A further study of the history of riverine warfare in the context of the newly established Naval Expeditionary Combat Command (NECC) will be done in order to finalize the C4ISR requirements.

CHAPTER III

Network-Centric Warfare and Distributed Operations (DO): This chapter will be a study of network-centric warfare in the maritime environment, the USMC DO doctrine, and how current technologies could be used to reach the disadvantaged user. This chapter will also focus on how the development of “last mile” communications is vital to the extension of NCW to the disadvantaged user.

This chapter will also expand a study upon Network Centric Warfare, the GIG, and various service NCW endeavors. The chapter will continue with a study of how Mobile ad-hoc networking (MANET) requirements complement the “last mile” communications’ architectures. The chapter will culminate in a study of IEEE 802.16 technologies, and how an adaptive wireless network topology using commercial-off-the-shelf (COTS) technologies will fulfill these MANET objectives.

CHAPTER IV

Fly-away Kit Construction: The combined COTS technology components to be used in the FLAK will be described in this chapter. IEEE 802.16 OFDM equipment, as well as the adaptive modular computing and sensor technology will be described, along with explanations of how the M-FLAK will be integrated into an overarching network architecture for NCW.

CHAPTER V

Field Experimentation: This chapter will focus on the field tests of the C4ISR FLAK, from the commencement of IEEE 802.16 testing at Pt. Sur California on December 2005 through the final integrated scenario tests of the completed FLAK in Chiang Mai, Thailand in May 2006. Measures of Effectiveness and Measures of Performance will be analyzed to study the performance of the IEEE 802.16 network topology, as well as all other periphery technologies in the M-FLAK.

CHAPTER VI

Conclusion and Recommendations: The culmination of this research will be examined in this chapter. There will be a focus on continued research areas which can be expanded from this thesis upon its completion.

II. MODERN RIVERINE WARFARE / MARITIME SECURITY

In order to understand the communications architecture necessary for these missions, an analysis of the current maritime theatre is needed. Also, the multiple US initiatives to enhance security in this domain must be studied as well. The over-arching maritime security strategies, in the context of the GWOT, will be examined, to include an analysis of the history of riverine warfare. This study of riverine warfare will establish the necessary doctrinal requirements for the mission parameters for the communications structures for modern integrated maritime platforms.

A. MARITIME SECURITY

1. Maritime Environment

The USS COLE (DDG 67) has become the prevailing symbol of the importance of maritime security in the prevention of terrorist attacks against high value maritime assets. Seventeen US Sailors were killed when the ship was attacked by a small boat on October 12, 2000, and the repairs to the stricken vessel rose to over $240 million USD before they were complete[11]. An Aegis guided missile destroyer such as the USS COLE is an important vessel in the US Navy's blue water fleet, contributing to all mission areas supported by the modern Carrier Strike Groups (CSG) and Expeditionary Strike Groups (ESG). The damage to the destroyer was significant, especially considering the low cost of fielding small boats laden with explosives.

[11] Downloaded from www.wikipedia.org on April 25, 2006

Figure 1. Damage to the USS COLE (DDG 67) after the October 2000 terrorist assault

Today, the global maritime environment is laden with threats well beyond those from traditional state actors. This trend is of increasing concern due to the growing vulnerabilities of a global economy dependent upon the modern maritime domain.

> Currently, 2.2 billion people live within 100 kilometers of a coastline; the maritime domain is home to 50,000 large ships that carry about 80% of the world's trade; and each year about 1.9 billion tons of petroleum is shipped by maritime transportation—approximately 60% of all the petroleum produced. Shipping industries around the world are taking advantage of the booming economy in China—shipping tonnage can barely keep pace with demand as Chinese exports grew 37% in 2004. In addition, a record 10.5 million people embarked on cruise ships in 2004, an increase of about 10% over 2003. Cruise industry analysts predict more than 11 million cruise passengers for 2005.[12].

Despite the significant level of trade, and the number of individuals traveling in the maritime domain daily, this arena is one of the most under-regulated portions of the world economy. The vulnerability of this region only becomes more apparent when these high-value targets become areas of significance in warfare.

[12] VADM Morgan and RADM Martoglio

In the current conflict in Iraq, MABOT and KAAOT, the two vital oil rigs in the Kwar Abd Allah (KAA) waterway[13], the Haditha Dam, and bridges on the Euphrates Rivers are all vulnerable to asymmetric strikes by insurgents, and must be protected.

> Maritime Security in the Gulf is critical for both the regional states and the global security. An estimated 15-16 million barrels of oil per day travel through the Straits of Hormuz to customers around the world, and any disruption of this traffic could have far-reaching effects on the global economy[14].

Current US and Coalition Forces have focused on the protection of these vital maritime choke points, but their deterrent presence has not prevented serious attempts by criminal pirate vessels from striking these targets with higher frequency.

> In the past year, even with the continued presence of Coalition Naval Forces in the Northern Arabian Gulf, piracy attacks have flourished, numbering 10 in 2005, when there were none in the previous years[15].

[13] Over $18,000 Dollars US in oil is passed through the Al Basrah oil terminals per second

[14] Russell, pg. 9

[15] Mukudun – Downloaded from www.iccwbo.org – International Chamber of Commerce (ICC). International Maritime Bureau (IMB) Piracy Reporting Center (PRC)

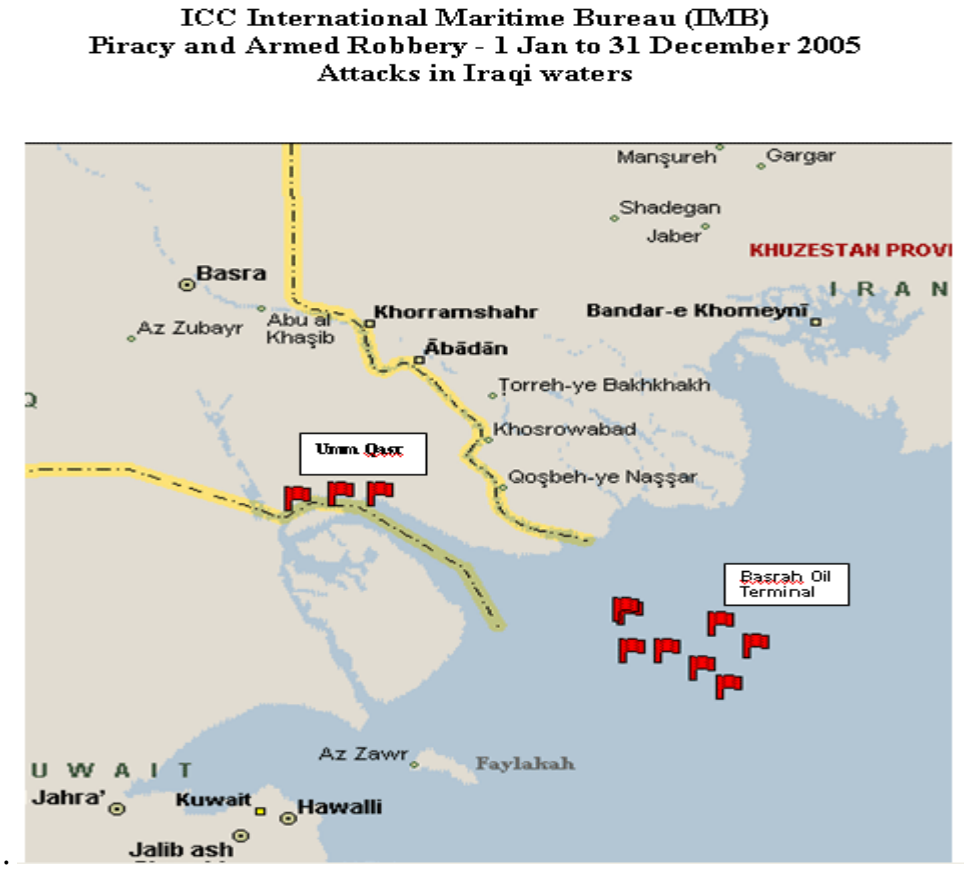

Figure 2. 2005 Pirate Attacks in the KAA

Global oil consumption is projected to increase to 120 million barrels by 2020[16]. Most of this oil will be shipped through vital ports on choke points around the globe such as the Straits of Malacca or the Suez Canal.

Two thousand and eight hundred ports now operate as nodes for the 230 million containers which pass through these hubs carried on approximately 46,000 ships. Thirty ports are now designated "mega-ports," defining them as critical nodes in the interdependent web of global commerce[17]. These economic hubs are severely lacking in protection from external, let alone, internal threats. For example, less than .05% of all containers entering US harbors are searched by customs and/or security forces[18]. This creates a considerable amount of maritime territory which is under minimal supervision,

[16] Mukudun – Downloaded from www.iccwbo.org – International Chamber of Commerce (ICC). International Maritime Bureau (IMB) Piracy Reporting Center (PRC)

[17] Ibid

[18] Reference need for the sheer levels of economic material moving in and out of US ports (MHLS?)

yet includes the majority of the water-borne economic material in the world. Terrorist organizations have been utilizing this "ungoverned space" to plan and execute operations against hubs of global commerce.

The October 6, 2002 Al-Qaeda assault on the French Tanker Limburg further highlights the type of targets maritime terrorists will seek to exploit. The devastating cost of the $45 million dollars in damage was further exacerbated by the severe environmental cost of 90,000 barrels of oil which spilled into the Gulf of Aden[19].

Figure 3. Damage to the French Tanker Limburg after a terrorist assault

These hubs and traffic flows must be protected in order to maintain the global economy; the US, as the world's largest economy and naval presence, cannot afford to remove itself from this endeavor.

2. Maritime Security Strategic Initiatives

The National Security Strategy required a shift in the intelligence community from the traditional Cold War endeavor of collecting intelligence on the Soviet Bloc to tracking a multitude of disparate and elusive sets of targets[20]. In order to accomplish this,

[19] Downloaded from www.wikipedia.org on April 25, 2006

[20] NSS and MHLS Reports

the traditional intelligence organizations must integrate more closely with the numerous law enforcement and regulatory agencies concerned with safe trafficking of commerce on the world's oceans. More importantly, these agencies must integrate with those civilian corporations which are traveling on the "front lines" of this less than conventional war.

Historically, "in surface transportation, timely information-sharing has been hampered by the lack of standard protocols to exchange information among federal, state, and local government agencies and private entities"[21]. This level of information-sharing is changing with the apparent increase in vulnerabilities being exploited by asymmetric threats on the world's waterways.

Databases are being linked in order to give all agencies and actors free and ready access to vulnerability assessments, timely indications and warnings, actionable intelligence, and operational data to the greatest extent permissible by law[22]. An Enterprise Architecture will link traditional intelligence[23] databases to non-traditional law enforcement and customs databases[24] until a total interagency fusion can be accomplished, resulting in complete and immediate information sharing[25].

This collection will still need to be done by the physical and remote presence of operators far from American soil. This will be the work of the modern riverine and maritime domain awareness forces of the NECC. Their collection of intelligence by a direct and indirect presence, reconnaissance and surveillance, and observation will complete the desired Maritime Domain Awareness (MDA) picture required by the NSS. Using Knowledge Management (NGKM), the mass of information being passed across the databases can be managed, and then disseminated to vector necessary platforms to interdict threats around the world.

The Secretaries of Defense and Homeland Security, building on the NSS, combined their strategic objectives for maritime security with four national objectives[26]. These national objectives are:

---

[21] O' Rourke CRS CG report – July 2004 – CRS-21

[22] USCG MHLS

[23] Defense, strategic

[24] Immigration, biometric

[25] USCG MHLS

[26] O' Rourke CRS CG report – July 2004 – CRS-21

- To prevent terrorist attacks and criminal or hostile acts
- To protect maritime-related population centers and critical infrastructure
- To minimize damage and expedite recovery from attacks within the maritime domain
- To safeguard the ocean and its resources[27].

The Navy and the Coast Guard are both working their C4ISR architectures in order to accomplish these mission requirements.

The Chief of Naval Operations (CNO), ADM Michael Mullen, has various strategic initiatives with the Global Maritime Intelligence Initiative (GMII) in conjunction with the Joint Force Maritime Component Command (JFMCC) and MDA to support interagency operations. As CNO, he has established the NECC at the Naval Amphibious Base Little Creek, Virginia on January 13, 2006 and has leveraged National Fleet Policy to coincide with the United States Coast Guard and the National Strategy for Maritime Security.

The Coast Guard's MDA requirements are being funded at higher levels, indicating recognition of higher priority. To enhance their current missions delineated in the Homeland Security Act of 2002, the following five areas of focus are highlighted:

1. Ports, waterways, and coastal security
2. Defense readiness
3. Drug interdiction
4. Migrant interdiction
5. Other law enforcement, including foreign fishing vessel incursions

The Coast Guard’s current forces need considerable enhancements to increase their ISR capabilities to the required levels on all of the United State’s maritime environs. Increases in the Homeland Security budgets have increased the ability of US national forces to achieve these goals. In a recent congressional report, the budget initiatives were

> It provides for critical increases in intelligence capabilities to enhance Maritime Domain Awareness (MDA). MDA will provide comprehensive, timely, and detailed visibility into events, conditions and trends in the

[27] O’ Rourke CRS CG report – July 2004 – CRS-21

> maritime domain that will assist Coast Guard Operational Commanders in the early detection of potential threats and optimizing allocation of operational assets.[28].

The Coast Guard will funnel these initiatives into the Deepwater project, Rescue 21, Automatic Identification System (AIS), and Response boat Medium Projects. These are necessary enhancements to the USCG forces, which have been hard-pressed to accomplish a significant portion of its missions prior to September 11th.

The overall governmental support for these initiatives is firmly entrenched within the recently published Quadrennial Defense Report (QDR). The QDR states several further areas of improvement which are required for all forces in the GWOT. All of these areas directly effect the transformation of maritime forces, and their integrated C4ISR network architectures:

- Human Intelligence to discern the intentions of the enemy
- Persistent Surveillance to find and precisely target capabilities in denied areas
- Capabilities to locate, track, and tag terrorists in all domains
- Special Operations Forces to conduct direct action, foreign internal defense, counterterrorist operations, and unconventional warfare
- Capabilities to help fuse intelligence and operations to speed action based on time-sensitive intelligence
- Multipurpose forces to train, equip, and advise indigenous forces,; deploy and engage with partner nations; conduct irregular warfare; and support security, stability, transition, and reconstruction operations
- Riverine capabilities to improve the ability of US forces to work with the security forces of partner countries to deny terrorist groups the use of waterways
- Joint coordination, procedures, systems, and, when necessary, command and control to plan complex interagency operations.
- Broad, flexible authorities to enable the United States to rapidly develop the capacity of nations to participate effectively in disrupting and defeating terrorist networks[29].

[28] O'Rourke, p. 2

[29] Quadrennial Defense Report, p. 23-24

The QDR also states the need for an enhanced maritime domain awareness capability to provide situational awareness and shared information on potential threats through rapid collection, fusion, and analysis[30]. All of these strategic requirements, as well as an assessment of their progress, must be integrated as seamlessly as possible. The blurred lines of the National Fleet concept's new mission parameters make this integration even more difficult to accomplish.

3. National Fleet Concept

The combined USCG and USN forces combine to become what is now defined as the National Fleet. Both of these forces will support the missions of the Department of Defense as well as the Department of Homeland Security. Their missions will blur, and become interoperable.

The current National Fleet Maritime Security Operations Model is designed to utilize the full range of the capabilities of the USN and USCG assets against the full spectrum of threats in the theatre today. These threats are:

- Human smuggling and slave trade
- Drug Trafficking and narco-terrorism
- Arms and monetary smuggling
- Passenger vessel protection
- Critical Infrastructure protection
- Mining of strategic ports
- High value asset protection
- Surveillance and broadcasting
- Border security threats
- Sea lines of communication security
- Weapons of mass destruction/effect
- Piracy[31]

[30] QDR, p. 27

[31] National Fleet Report

The USN will be utilized for high intensity conflict, focusing on maritime defense, while the USCG will focus on low-intensity conflict. The spectrum of maritime security will belong to the USCG and maritime defense will fall under the umbrella of the USN, but the defined lines which separated these missions are no longer exact. What is important to note is that in order to meld these defined mission lines, both sides of the National Fleet must become network-centric and interoperable in its communications.

4. International Maritime Security Initiatives

Maritime Initiatives have grown significantly in the new millennium. The International Maritime Organization (IMO) and the World Customs Organization (WCO) have published various initiatives to increase the level of maritime security to further protect the level of international commerce[32]. The December 2002 conference of the IMO amended the Safety of Life at Sea (SOLAS) and the International Ship and Port Security (ISPS) code, but both of these measures are voluntary, and require work by the member countries to enforce the standards.

The ISPS code has become a cornerstone of future surface shipping and commerce security. The IMO is managing a database of all shipping traffic from member nations of the 1974 SOLAS convention[33]. Although the IMO is producing guidance and managing the overall database, individual nation-states are enforcing their own technological adaptations within the code requirements.

The US has focused the additional codes to comply with SOLAS by adding the Automated Identification System (AIS), which fulfills the ID requirement of all ships over 300 gross tons[34]. The AIS is an important facet of blue-force tracking which is an integral part of all services' NCW concepts. The AIS will enable the US to fulfill ISPS code requirements for the military ships, and begin a move towards improving private steps to increase overall port security.

---

[32] O' Rourke CRS CG report – July 2004, CRS -13

[33] ISPS code data and IMO management of the database can be researched further @ www.imo.org

[34] O' Rourke CRS USN report – FEB 2006 – CRS-2. Small boats, which are under the 300 ton threshold, are a major security problem. Few fishing boats, for example, exceed these levels. A lot of ammonium nitrate can be placed into a crab boat, making small boast interdiction still vital despite these technological advances.

The WCO has a significant membership of 161 countries possessing 97% of the world's trade[35]. The WCO initiated the "Resolution on Security and Facilitation on the International Supply Chain" in June 2003, which attempts to standardize the data elements needed to identify high risk cargo and exchange information between exporting countries and importing countries customs services[36]. Still, like the IMO, initiatives require money in which to set-up and enforce. The US Congress has approved a "Maritime Security Trust Fund" to help countries improve their own port security[37].

Other initiatives such as the Regional Maritime Security Initiative (RMSI) were started, which was a Pacific Command plan to integrate PAC-RIM nations to cooperate on maritime security by focusing on joint patrols and information sharing, and are being implemented. As described on the intelligence global security website:

> The goal of RMSI is to develop a partnership of willing regional nations with varying capabilities and capacities to identify, monitor, and intercept transnational maritime threats under existing international and domestic laws.
>
> This collective effort will empower each participating nation with the timely information and capabilities it needs to act against maritime threats in its own territorial seas. As always, each nation will have to decide for itself what response, if any, it will take in its own waters.
>
> Information sharing will also contribute to the security of international seas, creating an environment hostile to terrorism and other criminal activities. Any RMSI activity in international waters will be in accordance with existing international law.
>
> Once a decision has been made to act against an emerging threat, maritime interdiction capabilities obviously will be required. In most instances, these will take the form of law enforcement or customs vessels, but military forces may be needed for more organized threats, especially on the high seas.
>
> RMSI will be a partnership of regional nations who are willing to contribute their resources to enhance maritime security. It is not a treaty or an alliance. Nor will the RMSI result in a standing naval force patrolling the Pacific.

---

35 O' Rourke CRS CG report – July 2004 – CRS -13

36 Ibid

37 Ibid, p. CRS-18

> The Proliferation Security Initiative, or "PSI" and RMSI are related, but the PSI is a global effort to stem the proliferation, by any means, of weapons of mass destruction and their delivery systems. PSI does not address other transnational threats. RMSI, on the other hand, will be focused on maritime transnational threats in the Asia-Pacific region[38].

These initiatives will be necessary to integrate in order to create a realistic "unblinking eye" of ISR.

Due to considerable opposition, RMSI was not able to be implemented because the cornerstone of the effort was to utilize US forces to patrol the sovereign maritime territories of other countries. This fact caused a "sudden death" for the initiative, but it still highlighted the importance of multilateral cooperation in achieving maritime security in regions like Southeast Asia. The loss of RMSI only re-enforces the need for C4ISR capabilities which can link the regional databases which already exist around the world.

Databases like the IMB's Piracy Reporting Center (PRC) in Kuala Lumpur must be integrated to track trends and intelligence on maritime piracy. As one of the growing asymmetric threats in the world, this global, and non-military, intelligence management of data will become vital to combat threats in the maritime domain. This also means the number of non-military forces which must be integrated into the maritime security architecture is considerable. Without these numerous international security agencies, there will be significant gaps in the information-sharing capabilities of these security forces.

5. Coalition Security Initiatives

The US global perspective on security initiatives must be balanced with the regional security initiatives of nation-states focused on regional maritime security. The proclaimed RMSI proposed by ADM Thomas Fargo in 2004 was an attempt to consolidate these numerous civilian, international, and military forces. ADM Fargo addressed the US congress with a plan to have US Navy/Marine Corps forces patrol the

[38] Downloaded from www.globalsecurity.org on April 30, 2006

Straits of Malacca. Although Singapore responded with support, both Malaysia and Indonesia responded to the US initiative with prejudice.

Malaysia and Indonesia have very different national security priorities from those of the United States. First and foremost, both of these countries list threats to their national sovereignty as the greatest danger to their national security. Maritime terrorism, piracy, and threats to their fishing fleets rank very low in comparison to other national security threats. This highlights the difficulty of implementing a regional maritime security agreement. Still, some countries have built upon the model of regional cooperation, realizing that trans-national efforts are required to solve global problems.

Singapore has initiated very important maritime security projects in the past decades, and has only accelerated these projects in the five years following the events of September 11th, 2001. These projects have led to very important improvements in the Singapore counter-terrorism infrastructure.

Singapore has ordered six of the French-multi-mission frigates which will extend the patrol footprint of the city-state out to the whole Straits of Malacca, the Indian Ocean, and the South China Sea[39]. Singapore is the only ASEAN member nation which is also a member of the 11-nation Proliferation Security Initiative (PSI)[40]. Singapore has also built a joint counter-terrorism center, which integrates law enforcement and intelligence for interagency data fusion[41].

Improvements in countries' information-sharing capabilities have led to countering maritime terrorist strikes before they can occur. For example, the Asian Regional Forum (ARF) improvements on sharing security data prevented planned Jemaah Islamiyh (JI) strikes against US vessels transiting the Straits of Malacca[42].

The ARF has coordinated Cooperation against Piracy, focusing on "regional cooperation to ensure that maritime criminals and pirates do not evade prosecution." This has defined a need for an "effective response to maritime crime requires regional

[39] Simon, p. 274

[40] Ibid

[41] Ibid

[42] Ibid, p. 278

maritime security strategies and multilateral cooperation in their implementation"[43]. The ARF is designing a counter-piracy initiative with the understanding of the obstacles:

- 80% of the world's maritime trade occur among the ARF nations
- The majority of the piracy in Southeast Asia occurs in coastal and archipelagic waters
- Cooperation between Navies and Coast Guards, shipping agencies, and port authorities[44]

To overcome many of these obstacles, the ARF nations are working on cooperative anti-piracy exercises, merchant marine training, and the designation of naval vessels for the prescribed shipping traffic lanes[45]. But even ARF still faces the "total consensus" voting style of the ASEAN nations.

Emerging security issues in Southeast Asia are:

- Piracy
- Smuggling
- Illegal immigration
- Trans-national Oil Spills
- Incidents at Sea
- Search and Rescue
- Navigational Safety
- Exchange of maritime Information
- Illegal Fishing
- Management of Resources in areas of overlapping claims[46]

All of these issues are essentially problems of a civil nature, but require the necessary intervention of military forces[47]. Therefore, military forces in the region must grow in their mission capabilities to deal with a much broader range of responsibilities and priorities[48].

---

[43] Ibid, p. 278-279

[44] Ibid, p. 279

[45] Ibid

[46] Valencia, Mark – The Asian Maritime Security Context, p. 11

[47] Ibid

[48] Piracy numbers since the MALSINDO patrols began 8 months ago have been extremely

Combined Task Force 150 (CTF 150) has developed out of the United States-led coalition enforcing the United Nation's Security Council resolutions 661 and 665. CTF 150 is currently commanded by a Royal Netherlands Navy Commodore, Frank Ord. The previous Commander was the French Vice Admiral Jacques Mazars. Overall, CTF 150 has involved participants from the navies of Germany, France, Pakistan, the Netherlands, the United Kingdom, and the United States. This model of coalition cooperation on the high seas is beginning to spread to remote positions in the maritime environs.

North Atlantic Treaty Organization (NATO) Operation Active Endeavour and Operation Active Effort are spear-heading similar multi-national efforts to patrol the Mediterranean to deny the forces of global maritime terrorism from assaulting the economic lifeblood between Europe, Africa, and the Middle East.

Figure 4. Insignia for the recently formed Malaysian Maritime Enforcement Agency

The Straits of Malacca, where more than fifty thousand ships pass each year carrying over ninety-five percent of Eastern Asia's crude oil (80% of Japanese crude oil; 50 % of international cargo shipping trade), has become an obvious vulnerability. Severe repercussions would result from a maritime terrorist attack upon shipping in the Straits. Since the vulnerability of shipping has been made abundantly clear by the annual increase is violent piracy assaults upon numerous ships in transit along the one thousand kilometer straight.

Currently, Norwegian Intelligence points to Al Qaeda control of 15-23 freighters, flying flags form the countries of Somalia, Tongal, and Yemen[49]

> Examples of emerging security networks include Black Sea Harmony in Eastern Europe, Caspian Guard in the Caspian Sea, and the counter-piracy initiative in the Strait of Malacca[50].

B. RIVERINE WARFARE

Riverine warfare strategic initiatives must be integrated with the overall maritime security strategy. Rear Admiral Donald K. Bullard of Naval Expeditionary Combat Command stated:

> The goal of naval thinking today, said Bullard, should be to "build awareness from the blue water to the green water to the brown water, in an integrated battle space." The maritime environment is a more complex matrix now. "You have to put riverine into this bigger picture," Bullard said. "It's not alone."[51]

Since the USN has not operated an active duty riverine force since the close of the Vietnam War, the history of riverine operations will be studied in order to establish mission requirement parameters for the communications architecture.

1. History of Riverine Warfare

The United States Navy has a long and distinguished history in riverine warfare. From before the Revolutionary War to the Global War on Terrorism (GWOT), US military forces have operated, both in peace and war, on "brown water"[52]. This history has been far from consistent, though, and has also been characterized by episodic periods, where riverine capabilities were completely removed from the USN inventory. Thomas Cutler, the author of Brown Water, Black Berets, states that:

---

[49] Russell, p. 10. The first US Amphibious Landing was actually performed by the US Army, with the US Revenue Cutter Service (Precursor to the USCG) during the Seminole War in Florida

[50] VADM Martoglio

[51] Rear Admiral Donald K. Bullard of Naval Expeditionary Combat Command– Eric Mills Seminar summation

[52] Dunnavent

> Brown water warfare has been used time and again, but on every occasion, once the necessity has passed, these capabilities were shelved and the Navy returned to "blue-water" operations[53]

This is extremely important because the USN has not operated a full-time and active Riverine command since the close of the Vietnam War.

Yet riverine operations have not been totally removed as a vital component of warfare and peace-keeping operations as they have been maintained by both the Army and the Marine Corps since the Vietnam War. The reason these forces were maintained was to conduct operations like counter-narcotics and nation-building. The functionality of riverine forces is that they control the one form of natural infrastructure used in third world countries, as expressed in the following passage:

> Rivers serve as lines for communications, transportation, and trade – can be more vital than roads in many remote regions – especially where there are more navigable rivers than roads[54].

Riverine warfare is as old as the country itself, and began with operations being conducted against the British during the Revolutionary War on the Delaware River[55]. It would continue throughout America's Indian Wars, and then again against the Barbary Pirates.

Gaining prominence during the "Jeffersonian Gunboat Era," riverine warfare reached a culminating period with the American Civil War, when US Naval monitors would work in concert with Ulysses S. Grant's Army to combat Southern Rebel forces along the Mississippi River[56]. Riverine warfare would take a back-seat to the global naval aspirations of the US during the latter half of the nineteenth century, but would slowly rise again once the US presence reached to the far corners of the globe.

The Chinese Navy traversed rivers for years of peace-time patrolling (continuing until the Japanese invasion of China) while exercising a form of US gunboat diplomacy. Large-scale navies are still the primary focus of nation-states even as the blue water focus

---

[53] Thomas Cutler, p. 23

[54] Wiley, p. 3

[55] Dunnavent, p. 9

[56] Dunnavent

shifted from battleships to aircraft carriers during World War II, prompting riverine forces to once again fall to the wayside of naval operations.

The Vietnam era would usher in another era of riverine warfare as the new technology and modern doctrine merged to establish a versatile multi-mission force to be deployed on the rivers of Southeast Asia. Most of the modern lessons of riverine warfare developed during the Vietnam War.

After the close of the Vietnam War, there was a reduction in the importance of riverine warfare, resulting in the USN deactivation of active riverine warfare commands, and a shift of its remaining Patrol Boat Squadron to Naval Special Warfare Reserve Commands. The USMC did not abandon its role in riverine warfare, and adapted FDI support forces to develop South American riverine forces for counter-narcotics missions[57]. The USMC forces trained the Bolivian Devils and established the Colombian Riverine Program[58]. These operations were successful, but were primarily under the auspices of Special Warfare, and were removed from the traditional aspects of Naval Warfare in the active duty Navy.

Throughout the history of naval riverine warfare, the classical tenets of the US doctrine which have developed are as follows:

- Harassing Fire
- Fire Support
- Riverine Amphibious Assaults
- Mobile Riverine Operations
- Direct engagements with other crafts[59]

These classical riverine warfare tenets are developed into three basic tactical necessities:

1) Harassing Fire / Interdicting Fire
2) Fire Support / Riverine Amphibious Landings / Mobile Riverine Forces
3) Direct Engagements with Vessels[60]

[57] Benbow, p. 22

[58] Ibid

[59] Ibid

[60] Ibid

The Vietnam Era expanded these missions by defining five specific mission areas which were required during riverine missions:

1. River Assault
2. River Patrol and Control
3. River Minesweeping
4. Special Operations Support
5. Fire Support from the Rivers
6. Consolidated Missions and Task[61]

The lessons from the history of riverine warfare are still the basic tenets of modern riverine warfare and security operations in peace-keeping missions.

The other important lessons from the Vietnam War are the necessity of interoperability with the logistics and aviation support elements. Riverine forces do not operate alone[62]. Close air support, directed by capable communications throughput, is vital to mission accomplishment. Whether directing US Close Air Support (CAS) during operations or directing the significant logistical support to the mobile riverine operators, communications must be maintained.

It is important to note the versatility of riverine forces in peacetime as well which has to integrate with the population.

> riverine warfare ... is not control of just the rivers and canals, it is control of the whole area, and that takes more than just boats," said Captain Hock, "You have to become part of the culture. You have to integrate[63].

Modern responses to humanitarian disasters will require not only a military response, but a mixed governmental, non-governmental, and volunteer collaboration. A capable and interoperable riverine force would have been extremely useful during the humanitarian efforts undertaken by CIV-MIL forces during Hurricane Katrina Relief Missions.

---

[61] Benbow, p. 14-16

[62] While Riverine craft are the centerpiece of any Riverine Operation, they cannot carry out any significant riverine missions by themselves. Nor are they single-service. When the Army started getting effective at interdicting the shore threads of the Ho Chi Minh trail, the coastal munitions smuggling business took off. In response, USCG deployed three squadrons of patrol boats, backed by high endurance cutters. The patrol boats had slightly augmented crews and the .50 cal on the forecastle got an 81mm mortar piggy-backed on it. And the boats were repainted grey. When the drawdown occurred, all these WPBs were turned over to South Vietnamese Navy. - Benbow, p. 21.

[63] CAPT Kwan Do (ret) of the Vietnamese Navy – Eric Mills Seminar summation

2. Current Riverine Environment

In analyzing the 60 non-integrated countries where Foreign Internal Defense (FID) missions are to be executed by deployable US riverine forces, almost every one of these countries fall along the equator. [64] The median income among these countries averages $2450 US dollars per year, and contains 30 percent of the world's waterways[65]. This means the US can expect to deploy these forces to an extremely hot (desert or jungle) and generally poor environment to work alongside coalition host nation (HN) forces with very little communications capability. Also, this means military forces which are lacking an infrastructure to support difficult to maintain systems when US forces are not invited, and can only provide technical assistance through advisors.

3. Modern Riverine Doctrine

Riverine Warfare is inherently joint, often combined, and always complex, requiring continual close combat and the management of combined arms[66]. The main missions to be undertaken by the modern US riverine force are:

- Security Assistance
- Counter-Insurgency (COIN)
- Global War on Terrorism (GWOT)
- Major Combat Operations (MCO)[67]

Traditionally, the riverine maritime theatre has been managed separately from the overall US blue water forces. The maritime domain is directly related to maritime security, and must be treated as such in strategic planning.

There are 60 countries which are currently considered to be the modern non-integrated gap. In these countries, the US may be called upon to conduct FID operations in support of the GWOT and where there are a collective 201,000 kilometers of

[64] Benbow, p. 42

[65] Ibid

[66] In the Vietnam War, more USCG sailors were killed by friendly fire from USAF forces. Benbow, pg. 1.

[67] Benbow CNA Report – "Renewal of Navy's Riverine Capability: A Preliminary Examination of Past, Current, and Future Capabilities

waterways and 21 river deltas[68]. These riverine environments are all significantly different and robust communications capabilities will be required to compensate for these differences. One of the key obstacles to overcome this is the communications interoperability with indigenous para-military and military forces, which must be connected with US riverine operators[69]. The necessary parameters for these communications links must be defined.

It has been a number of years since a US joint operational doctrine for riverine tactics has been updated. Historical lessons from experiences of operators are the sole source of lessons learned from which a new doctrine can be devised.[70]. Therefore the historical lessons from riverine warfare must be used as the guidelines for the future.

According to the CNA study on "The Future of the Navy's Riverine Capability" published in March 2006, the following requirements for ISR and C3 are defined as follows:

ISR

- Employ visual and electronic sensors
- Employ human exploitation team (HET) to collect local HUMINT
- Coordinate with Rotary-wing (RW) recon support for river patrol

C3

- Conduct joint mission planning, including employment of joint intelligence products
- Provide C2 organic fires and maneuver
- Integrate direct fires and maneuver with adjacent GCE
- De-conflict organic direct fires with friendly forces and facilities in the vicinity (IVO) waterways.
- Provide initial terminal guidance for helo landing zones (LZ) IVO waterways

[68] Ibid – the non-integrated gap of countries is characterized by The Pentagon's New Roadmap: War and Peace in the Twenty-first Century (G.P. Putnam's Sons, 2004). It refers to the countries outside of the core which have not bonded into mutually assured dependence through integration into the world's economy. The gap includes countries which can take a path towards integration, or in opposition to globalization.

[69] Benbow, p, 21

[70] Joint Riverine Doctrine was last refined

Other Supporting Information Operations (IO) mission requirements

- Conduct IO IVO waterways[71]

These mission parameters match much of the informational requirements for other DO missions in the current military architecture. The non-C4ISR mission capabilities revolve around similar operational mission parameters, and simply focus on the area of

The CNA report focuses further on what it considers to be obstacles to achieving a superior C3 environment in this field of operations; primarily foliage obstruction, communications relay, chain of command structure, and weather conditions[72].

C. NAVAL EXPEDITIONARY COMBAT COMMAND (NECC)

On October 1, 2005, the NECC was created by the USN, and the future naval riverine force was planned as one of its elements[73]. The other elements include other previous organizations: the Naval Coastal Warfare Squadron (NCWS), Explosive Ordinance Disposal (EOD), Mobile Diving and Salvage, Naval security, Naval Expeditionary Construction Battalions, and other specialized deployable commands[74]. According to RADM Donald K. Bullard, the NECC was created to "fill the gaps in security between the big ships that patrol the deep blue waters and the troops ashore that are exploited by the Cole attack" [75]

The Riverine Warfare Group (NRG-1) will deploy three river combat forces of twelve boats each[76]. Each of these 12 boat teams will be split into four different groups, each manned by five-man crews, enabling a port and starboard rotation during surge operations. These riverine groups will be deployable around the globe, and thus making the Combatant Commanders (who may have considerable riverine mission requirements) compete for their availability.

It's no coincidence that the dual missions of maritime security and riverine combat are co-located in the same recently established command in the US Navy. The

[71] Benbow, p. 5

[72] Ibid, p. 58

[73] Ibid, p. 7

[74] Ibid

[75] Hettna – "Navy Takes on Terror"

[76] Ibid

dual nature of conducting military and constabulatory operations in both a peacetime and wartime context has made small boat operators, whether in the USCG, the USN, or a coalition ally operating with them, mirror images of each other.

Although no specific mission set of force construct has been defined, the NECC Riverine Group has established their operational subset to bring area control, counter-piracy, interdiction, insert/extract, fire support coordination, and identify/locate/destroy missions firmly and officially[77]. These missions will become the cornerstone of modern riverine and maritime security initiatives.

The NECC will deploy its riverine forces to support OPERATION: IRAQI FREEDOM by 2007 in order to replace the USMC riverine forces conducting maritime security missions[78].

Also deploying in 2007 under the NECC command structure will be the Naval Coastal Warfare Squadron Five (NCWS 5), which will focus on the maritime security mission[79]. The NCWS will focus on missions in littoral areas, like the Al Basrah terminals in the NAG, counter-piracy along the Horn of Africa, and South Korean littoral patrols along the Demilitarized Zone on the 38th Parallel[80]. The NCWS will also fulfill missions in support of law enforcement and the USCG.

The communications interoperability which must be achieved by the NECC and its multitude of multi-mission small boat squadrons will require significant bandwidth and distance links despite numerous different architectures and topologies being structured in the "last mile." A breakdown on the many different crafts which must be linked, from current ships in the US and coalition force to the up and coming NECC craft, will highlight that modularity is vital to overcoming this obstacle.

D. MARITIME AND RIVERINE CRAFTS

It must be stated that speed and mobility will be critical facets of riverine warfare doctrine, especially concerning the high speed small boats in the current US Joint inventory. As USMC Major Ivan Monclova, USMC, Deputy Naval Mission Chief,

[77] Mills

[78] Benbow, p. 7

[79] Hettna – "Navy Takes on Terror" – Monterey Herald

[80] Ibid

Bogota, Colombia, and USMC Representative to the Colombian Marine Corps stated about his experiences in riverine warfare: "Enemy sniper fire is death on wheels. If you're not moving fast, you're definitely a target"[81]. As shown by the chosen crafts for the modern riverine warfare forces, speed is vital to doctrine, and therefore, communications must take this speed into account.

In final, it is important to note the Earth is 75 percent water, and thus it is physically impossible for these boats to patrol every section of the globe's oceans simultaneously. This "boring of holes in the ocean" is pointless without an integrated communications architecture to enable these ships to operate in an interoperable manner. Information systems which can focus the multiple aviation assets necessary to patrol are necessary. The following analysis of small boats will focus on the kinematics of interdiction boats, and the logistical placement of the modular maritime fly-away kits.

1. Rigid Hull Inflatable Boats (RHIB)

The Rigid Hull Inflatable Boat (RHIB) is the standard operating craft for maritime security and MIO operations. The Naval Special Warfare (NSW) RHIB is rugged and can maintain a 200 nautical mile range at 32 knots with a 45 knot top speed[82]. The NSW is C-130 transportable and can carry either 3200 pounds of payload or eight passengers. The RHIB also possesses an antenna array which stands close to ten feet in height, ideal for the placement of FLAK IEEE 802.16 antennas.

[81] Mills

[82] Downloaded from www.globalsecurity.org on April 22, 2006

Figure 5. Naval Special Warfare RHIB

2. Special Operations Craft – Riverine (SOC-R)

The Special Operations Craft – Riverine (SOC-R) is the new riverine warfare craft utilized by the US Navy. Comparable to the RHIB in size, speed, and payload capacity, the SOC-R has few definable characteristics which would require a distinct change in testing parameters concerning the addition of MANET communications architecture onto the craft[83].

Like the NSW RHIB, the SOC-R is also produced by US Marine, INC. The SOC-R Cyclone is a replacement for Vietnam-era PBR-style riverine combatant craft.

[83] The SOC-R possesses comparable Key Performance Parameters (KPP) to the RHIB – C-130 transportable, 33 foot length, 200 nm range

Figure 6. Naval Special Operations Craft – Riverine (SOC-R)

3. Small Unit Riverine Craft (SURC)

The SURC is the USMC's vehicle to conduct Military Operations in the Riverine Environment (MORE)[84]. Designed to achieve speeds of close to 40 knots, the SURC is capable of beaching itself for land-based assaults. The SURC is transportable by both the CH-53 Helicopter and MV-22 Osprey. Also, the SURC has a modern communications suite, capitalizing on advanced digital technology and the use of the US Army's Combat Radio Network (CRN)[85].

[84] www.globalsecurity.org/military/system/ship/surc/.com

[85] The CRN will be discussed further in Chapter III

Figure 7. USMC Small Unit Riverine Craft (SURC)

The SURC is designed to carry 13 to 18 marines, the equivalent of a squad. The SURC-E is planned to be a combat support element for the standard SURC, which will operate primarily as a troop carrier for a rifle squad. The SURC is designed specifically for another vital aspect of riverine warfare: going ashore.

As previously stated by various officers and sailors who experienced brown water warfare in the Vietnam Era and counter-drug operations in SOUTHCOM, placing boats on the water without the ability to go ashore simply creates asymmetric targets for the enemy. As USMC Major Ivan Monclova stated at the Naval Institute conference on riverine warfare:

> "You have to get off the boat." Civilian assistance—providing medical aid, delivering essential supplies, and any other type of goodwill initiatives—has to be perceived as a crucial part of the mission. Not only are you doing a good deed, observed Monclova, but "you're taking those villages away as bases of operations" for the bad guys[86].

[86] Mills

The QDR highlights the recent addition of over 3700 personnel to the current military force for the purpose of conducting civil affairs and psychological operations[87]. These forces will be required to operate in regions with minimal logistical and transportation support. This means their missions will become closely integrated with the missions of the NECC.

In Vietnam, the use of a US Navy riverine advisory effort enabled increases in indigenous riverine security capabilities. This is much like what is envisioned for the international security cooperation programs desired by the US and its allies today[88]. In many of the countries where civil-military operations will occur, rivers are the sole form of transportation and communication[89].

4. Special Operations Craft – MK V PEGASUS

The MK V Pegasus SOC is the largest special operations crafts operated by NSW. At 82 feet, the MK V is three times as long as the Cyclone and the NSW RHIB. The MK V also possesses much greater range than the other two small boats, yet is still small enough to be transported by two USAF C-5 aircraft within forty-eight hours of notification.

Figure 8. Special Operations Warfare Craft MK V Pegasus

[87] QDR, p. 5

[88] Benbow, p. 13

[89] Burma currently maintains no East to West roads – only rivers – Burma's Armed Forces: Power Without Glory Selth, p. 4

The communications suite of this craft is much more robust than those onboard the Cyclone and RHIB. Advanced navigation, radar, as well as radio and satellite communications complements these already versatile military craft.

5. USCG Harbor Security and Motor Life-Boats (Mlb)

Figure 9. USCG Harbor Security Patrol Boats

The United States Coast Guard maintains the constabulatory role in the US continental littorals. Furthermore, the USCG has expanded its role in maritime security since the events of September 11th. With its transfer to the Department of Homeland Security, the USCG has expanded its small boat inventory to enhance its mission capabilities. The USCG's motor life boats (MLB), and other security boats are easily adaptable to modular C4ISR communications suites.

Figure 10. USCG Motor Life Boats (MLB)

6. Coalition Forces

As stated previously, the sheer size of the Earth, combined with the fact that the globe is mostly covered by water, ensures that even combined, USN and USCG ships have little hope of providing continuous coverage of every nautical mile of blue water. By the same logic, US riverine and maritime security forces cannot cover all littoral and riverine theatres. The future of riverine and maritime security hinges on the various regional alliances to maintain security.

CTF 150 is a coalition maritime security force which operates in the waterways of the Central Command (CENTCOM). CTF 150 is a composite force operating numerous naval vessels in order to maintain maritime security in the Persian Gulf. Under European Naval command, US forces routinely operate security missions throughout the region.

MALSINDO (named for the Malaysian, Singapore, and Indonesian navies) patrols the Straits of Malacca. In 2004, in fear of maritime terrorism and growing piracy, ADM Fargo (PACOM) offered US Navy and Marine Corps support for patrols in the Straits[90]. Those patrols were accepted by Singapore, but firmly denounced by Indonesia and Malaysia, who desired to patrol their own territorial waterways[91].

Figure 11. Indonesian Frigate patrolling the Straits of Malacca

90 www.wikipedia.org/RMSI/

91 Ibid

The Indonesian Navy, despite opposing US forces patrolling the Straits of Malacca directly, has been receptive to information-sharing, to include the addition of US collection technology on their crafts[92]. The Malaysian Maritime Enforcement Agency (MMEA) is considering a near term partnership with the Naval Postgraduate School regarding technology initiatives which can be integrated into their emerging capabilities.

7. Junk Force Craft

In the Vietnam War, a large portion of the riverine force were "Junk Force" ships, commercial craft "deputized" to operate as interdiction patrol ships in conjunction with US and Vietnamese forces[93]. These forces greatly increased the number of ships available to patrolling forces.

In the current QDR, the importance of allied countries "policing themselves" to counter the threats within their country is strongly emphasized[94]. Before fully interoperable maritime forces can be developed, interaction with US Forces in an advisory role must be developed. In many of these countries, the first vessels which will be available to these governments will be converted civilian craft. With a proper enhanced military communications suite, they can fulfill the roles of intelligence and supporting patrol craft. In other words, immediate action to quell the disorder in the country could be taken before US forces could be fully deployed into the theatre[95].

E. SUMMARY

The requirements placed on the maritime security and riverine forces of the US multi-service small boat forces and their coalition counterparts, require a survivable, modular, secure, and manageable C4ISR network topology architecture. This topology must enhance the capability of their sensor-to shooter timeline across a layered global maritime domain.

---

92 www.globalsecurity.org/RMSI

93 Cutler, pg. 26

94 QDR, pg. 17

95 Ibid

THIS PAGE INTENTIONALLY LEFT BLANK

III. MOBILE AD-HOC NETWORKING

This thesis expands on the work of previous students at Naval Postgraduate School (NPS). IEEE 802.16 technologies have been studied in the context of the USMC doctrine of Distributed Operations, Ship to Operational Maneuver (STOM), and USCG constabulatory missions in Homeland Security. Furthermore, the study of FLAKs in order to increase the modularity of communications has been initiated by Capt Dwayne Lancaster, USMC, in his thesis studying the importance of Fly-away kits for responses to humanitarian disasters.

This research capitalizes on the efforts of these NPS graduates in order to apply these applications to C4ISR support in riverine warfare and maritime security.

A. NETWORK-CENTRIC WARFARE (NCW)

The Office of the Secretary of Defense describes Network-centric warfare (NCW) as an emerging theory of war in the Information Age[96]. The term encompasses the "combination of strategies, emerging tactics, techniques, procedure, and organizations that a fully, or even partially networked force can employ to create a decisive war-fighting advantage[97]. This information advantage is that:

> NCW generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, high tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, it translates information advantage into combat power by effectively linking friendly forces within the battle-space, providing a much improved shared awareness of the situation, enabling a more rapid and effective decision-making at all levels of military operations, thereby allowing for increased speed of execution[98].

Although the term NCW has existed since 1998, the military formally adopted the concept into its Joint Vision 2020, when it established the key elements of a transformed networked force. The modern vision of NCW involves the network itself to be the

[96] NCW, p. 3

[97] Ibid

[98] Ibid, p. 4-5

centerpiece of NCW, as opposed to the traditional legacy system platform-centric networks of military history. The key elements to be taken from the US military's future adaptations of NCW are:

- A robustly networked Force improves information sharing
- Information sharing enhances the quality of information and shared situational awareness
- Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command[99]

Current initiatives in the development of NCW forces have not been refined into a routable architecture.

Although NCW has existed in a partial manner for some time in the USN, with its adaptations of JTIDS and GCCS-M, these technologies have been centered on the larger carrier based fleet deployments. Furthermore, these are not routable networks, and cannot be integrated into an internet to share data. NCW has not extended down to remote users like small boat operators. Still, the long-term goal of all US forces is to be linked together in an internet that will collect, manage, and disseminate all data, to include targeting information, from every sensor to every shooter. The centerpiece of this accomplishment of NCW will be in the Global Information Grid (GIG).

1. The Global Information Grid

The GIG is the internet designed for the Department of Defense (DoD) and is defined as:

> The globally interconnected, end to end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to war-fighters, policy makers, and support personnel[100].

[99] DoD Report to the US Congress of NCW

[100] DoD Instruction 81001p

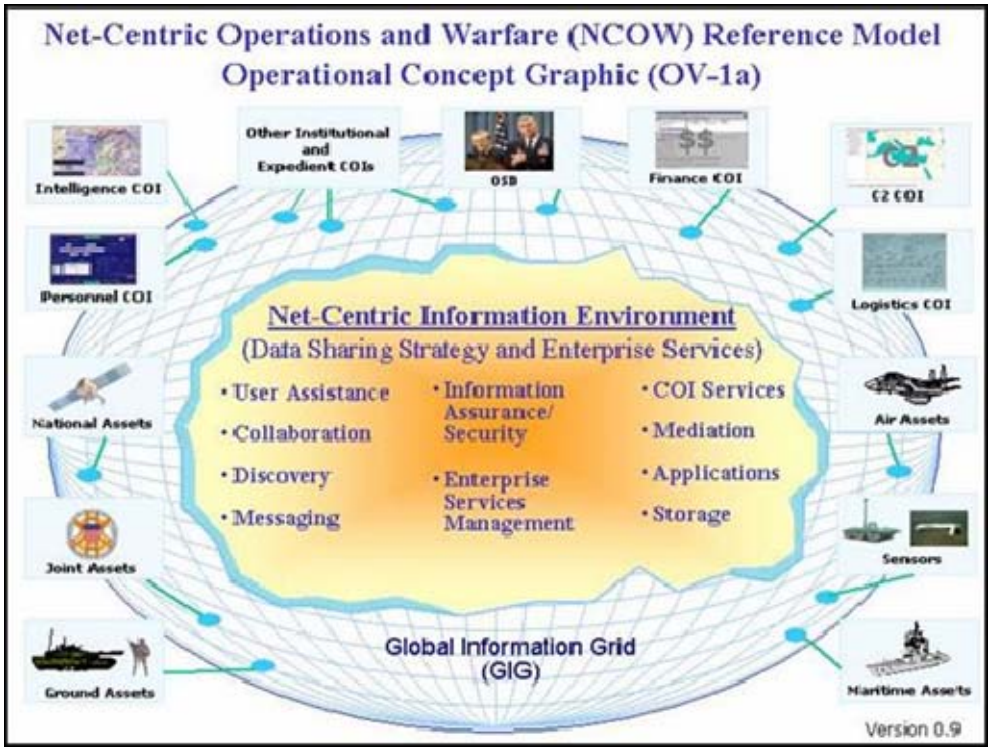

Figure 12. Network-Centric Warfare diagram of the Global Information Grid (GIG)

In other words, all communications capabilities, personnel, and equipment related to the defense of the United States, whether utilized in peace or war, is to be integrated seamlessly into the GIG. Tactical radios in the field to strategic intelligence satellites are all to become inter-operable. To make the goal slightly more complex, all coalition and allied forces, as well as non-DoD users and systems supporting the national security structure, must be integrated as well. In JV2020, the GIG is listed as the key to the future military's "strategic agility" in information operations[101].

The Global Information Grid Bandwidth Expansion (GIG-BE) is a recent endeavor to increase the throughput of the GIG for all of the users. With the number of applications, processes, and users constantly increasing and lending pressure to the demands of real-time bandwidth, there has been a push to focus on increasing the number of bits which can be transferred between modular users. With Voice over Internet Protocols (VoIP), digital security IP cameras, higher Graphical Information Systems, and GPS, and greater numbers of users linked in, the need for increased bandwidth grows at an accelerated rate.

[101] JV 2020, p. 9

There are obstacles to fully achieving the GIG, and the most prominent is the difference in technologies adapted by the various militaries. The GIG is a DoD internet, and its focus is to pass data down to all services. Each military is working to link together their service-specific NCW endeavors to the GIG, much like the differing technologies utilized in the internet interoperate over similar protocols.

The GIG is far from complete, and the end systems which will be implemented onto this DoD internet, requires specific measures in order to design the topology correctly. The strategy for the implementation of a GIG requires:

- LAN
- Terrestrial WAN
- Radio-WAN
- End-to-end security measures
- End-to-end management
- Next generation protocols[102]

The application of these requirements will be addressed further, and re-visited as standards when the specific thesis technology is addressed later in the thesis.

2. Usn/Usmc – FORCEnet

FORCEnet will be the communications structure behind SeaPower 21, the triumvirate strategy for the transformation towards future naval operations. Sea Power 21 entails Sea Strike, Sea Basing, and Sea Shield. Sea Strike entails the offensive capabilities while Sea Shield entails the defensive. Riverine and maritime security exists in both of these. Sea basing is focused on the support to the other two pillars of Sea Power 21.

> We often cite asymmetric challenges when referring to enemy threats, virtually assuming such advantages belong only to our adversaries. "Sea Power 21" is built on a foundation of American asymmetric strengths that are powerful and uniquely ours. Among others, these include the expanding power of computing, systems integration, a thriving industrial base, and the extraordinary capabilities of our people, whose innovative nature and desire to excel give us our greatest competitive advantage[103].

[102] Buddenberg

[103] ADM Vern Clark – Proceedings article

The connecting glue of these three portions of Sea Power 21 and the three supporting portions will be FORCEnet.

Figure 13. FORCEnet 21 as an integrated composite of Sea Power 21

FORCEnet is designed to be the NCW of the combined Navy-Marine Corps team, architecting warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force[104].

> ForceNet will provide the architecture to increase substantially combat capabilities through aligned and integrated systems, functions, and missions. It will transform situational awareness, accelerate speed of decision, and allow us to greatly distribute combat power. ForceNet will harness information for knowledge-based combat operations and increase force survivability. It will also provide real-time enhanced collaborative planning among joint and coalition partners[105].

ForceNet Impact

- Connected warriors, sensors, networks, command and control, platforms, and weapons
- Accelerated speed and accuracy of decision
- Integrated knowledge to dominate the battlespace

[104] Sea Power 21: Projecting Decisive Joint Capabilities by Admiral Vern Clark, U.S. Navy. Proceedings, October 2002

[105] Ibid

ForceNet Capabilities

- Expeditionary, multi-tiered, sensor and weapons grids
- Distributed, collaborative command and control
- Dynamic, multi-path and survivable networks
- Adaptive / automated decision aids
- Human-centric integration

> "Sea Power 21" will be implemented by a Global Concept of Operations that will provide our nation with widely dispersed combat power from platforms possessing unprecedented warfighting capabilities. The global environment and our defense strategy call for a military with the ability to respond swiftly to a broad range of scenarios and defend the vital interests of the United States. We must dissuade, deter, and defeat both regional adversaries and transnational threats.
>
> The Global Concept of Operations will disperse combat striking power by creating additional independent operational groups capable of responding simultaneously around the world. This increase of combat power is possible because technological advancements are dramatically transforming the capability of our ships, submarines, and aircraft to act as power projection forces, netted together for expanded warfighting effect.

The plan for FORCEnet is a smaller scale, yet comparable vision, to the goal of the GIG: an impact on distributed operations around the globe. This defines itself in the intended Global Concept of Operations to be implemented through the technology:

- Widely distributed, fully netted striking power to support joint operations
- Increased presence, enhanced flexibility, and improved responsiveness
- Task-organized to deter forward, respond to crises, and win decisively

This Global Concept of Operations fits well within the ideal of the GIG, and the multiple mission parameters which NCW is designed to achieve in the GWOT-operational multi-mission capable naval forces. Unfortunately for the simplicity of this vision, it requires interoperability with other military, civilian, and law enforcement actors in the GIG, as well as outside of its architecture.

This vision of the FORCEnet, since it will complement the missions of the National Fleet, must be defined alongside the Integrated Deepwater 21 System.

3. USCG – Deepwater

The Integrated Deepwater System 21 (IDS) is the USCG's answer to NCW. IDS is designed to provide the capability to:

> Harness the power of an interoperable network to improve in all mission areas – enabling distributed operations and the sharing of information quickly and seamlessly across a wide range of units. Improved intelligence capabilities are true force multipliers in acquiring higher levels of actionable intelligence information allow commanders to make better informed operational decisions, manage risk wisely, and employ forces more[106].

Much like FORCEnet, IDS-21 is a focused on an improvement of C4ISR equipment, networks, and doctrine in order to refine a sensor to shooter mesh, which can reduce the decision-makers time concerning adversaries in the maritime environment.

Figure 14. Deepwater Assets to be integrated into the full NCW architecture

4. DIGITAL DIVIDE

The "digital divide" is the division of communication assets at the strategic and operational level versus the tactical operator. The infantry soldier in the field is

[106] Downloaded from www.uscg.mil/deepwater/ on April 24, 2006

disadvantaged in his ability to link to the new technologies which enable NCW. It is the "last mile" connection which has not been achieved through current networking capabilities in the military.

Currently, the US has substantial communications at the division and brigade level. For the Navy, this means adequate communications at the carrier and command ship level. For further connections to the dismounted infantryman or boarding officer, two steps must be accomplished.

The first step is to connect from the division/brigade level down to the last vehicle. This is the focus of current MANET research. The attempt to establish standard Radio-WANs through various technologies in order to enhance NCW in the military has been inconsistent and episodic at best. Various research initiatives have been implemented with the intention of linking these remote users, but none have been successful.

The second step includes the connection from the brigade down to the company level down. Ashore, it is the dismounted infantryman. Afloat, it's the boarding officer that has stepped off his boat. This represents both a major and minor problem. The minor problem is to allow the network to function; the major problem will be to provide electrical power to the components that accompany the dismounted infantryman (current battery technology is too limited).

Closing this digital divide is the primary goal of Mobile Ad-hoc Networking (MANET) research today in the military, as well as in the commercial world. It is to this disadvantaged user that the focus of the communications links in this thesis will focus.

In a military sense, the digital divide exists primarily between the Major Subordinate Commands (MSC) and the small maneuvering forces which operate OTH and NLOS. For the maritime environment, these include riverine operators, small boats conducting VBSS, and maritime security missions. These on the move operators have been separated from the military communications architecture by systems deficiencies throughout their history, and only recently have been connected through MANET.

B. MOBILE AD-HOC NETWORKING (MANET)

A MANET is a self-configuring network of mobile routers (and associated hosts) connected by wireless links—the union of which form an arbitrary topology[107]. MANETs are devised to require minimal configuration, be quickly deployable, and suitable for emergency situations like humanitarian disasters. MANETs can be operated in conjunction with the internet, or as a stand-alone network[108].

In recent years, with the advent of IEEE 802.11 ad-hoc networking, networks without wireless access points (WAP) have been adapted into MANET research studies. This has enlarged the techniques of the adaptations of new standards of wireless transmission.

Current deployed MANETs in the military include the Joint Tactical Radio System (JTRS) and the Near Term Digital Radio (NTDR). JTRS is a joint US-NATO research project on the development of software-defined radios (SDR). JTRS is a layer 3 solution and operates within the routers. Meanwhile, NTDR is the US Army's MANET for disadvantaged operators in ground warfare. JTRS is the current standard in military MANET research, attempting to culminate ground, airborne, and maritime radios with multiple waveforms operating on each radio[109].

MANET research has been devised from many different directions. Some schools of thought have focused on adapting digital / analog data transformers to take advantage of digital bandwidths and analog RF propagation. Other avenues of thought have worked within the IEEE digital transmission standards, adapting wireless networking technology to tactical applications. Both of these directions have their advantages. The following recommendations are based upon lessons learned in MANET technologies.

MANET must be architecture-oriented. In other words, design of the network infrastructure should come before any focus should be placed on the secondary systems on the network. "All information systems are made up of sense, decide, and act end

---

[107] Downloaded from www.wikipedia.org on April 25, 2006

[108] Setting up a stand-alone network in NCW would be pointless, despite the capability existing with the technology.

[109] www.globalsecurity.org/JTRS/ Comparisons in previous research have used JTRS as the benchmark for comparison of the capabilities of 802.16 networks in previous thesis conducted at NPS. This study will not focus on this study in a any more depth. This thesis will expand on the superiority of 802.16 network topologies over the JTRS model of network architecture.

nodes" and the internet which connects them together. End systems are not connected to each other, but instead to a system within the platform[110]. This is accomplished in a LAN by a router. Therefore, a simple design adjustment to a network requires only a router re-programming.

The seven layer OSI model of network architecture is a standard applied to all network design and architecture[111].

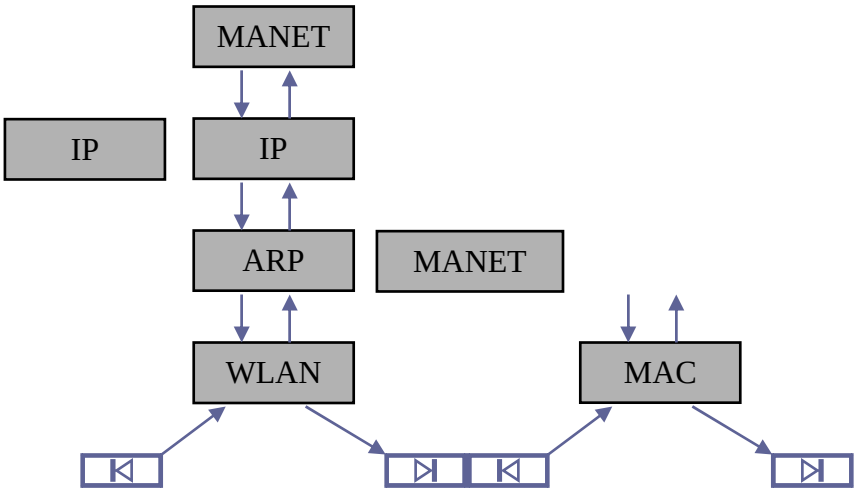

Figure 15. MANET Architecture versus the OSI model architecture

The future of MANET in the military should revolve around the application of these rules to the design of any future architecture. Fortunately, commercial standards concerning the implementation of parameters like this have already been built into commercial wireless network protocols.

Two basic architecture principles must be integrated into any MANET design. The first principle is the Platform-Level LAN. This means that all end systems on the network are connected to the platform's LAN. Another way to interpret this is as follows: All information systems are made up of sense, decide, and act end nodes (known as end systems in internet-speak), and the network that connects them together. Complexity is simply these same elements together with nesting and chaining.[112]

[110] Buddenberg – "A Perspective on Mobile Communications" Dec 2005

[111] Douglas Comer, p. 48

[112] Buddenburg, "Objective, Architecture and Strategy for Network-Centric: A Perspective on Mobile Communications", p 2

This means that every periphery technology will only speak to the LAN, and require a different link in order to connect to the periphery technologies on other platforms.

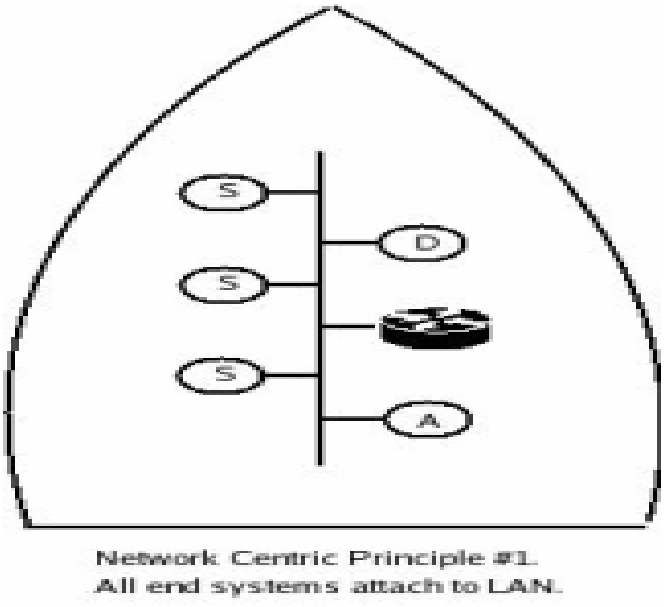

Figure 16. Information System Principle #1

Since the LAN maintains the connectivity between the end systems, they do not connect to anything outside of the platform. They are connected to other platforms through the router on the LAN. This is where the second principle of MANET architecture becomes important.

The second principle of MANET architecture is the WAN, where both radio and terrestrial, can be viewed as a cloud with routers at the border[113]. It is important to note that this is the overarching architecture planned for the full integration of the GIG-BE, where router links between periphery technologies will connect through routers on platform oriented LANs.

[113] Ibid, p. 3

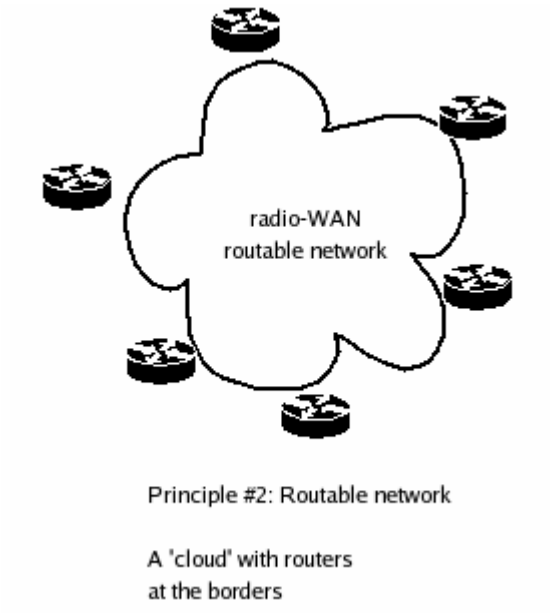

Figure 17. Information System Principle #2

Currently, a COTS communications technology exists which could fulfill the role of linking mobile military units in this manner. With a focus on the Layer 1 and 2 sections of the OSI model, it would fulfill the linkage between platform-centric LANs with end systems[114], as well as function as the Radio-WAN routable network between these platform-centric LANs[115].

C. IEEE 802.16 [116]

1. IEEE 802.16 Background

IEEE 802.16 is a wireless networking standard published by the Institute of Electrical and Electronics Engineers (IEEE)[117]. Its purpose is to provide low-cost compatible and interoperable standards for the design of broadband wireless equipment

[114] Ibid,, MANET Principle #1

[115] Ibid, MANET Principle #2

[116] A significantly more in-depth study of 802.16 was completed at NPS by USMC Captains: Robert Guice and Robert Munoz in their thesis: "IEEE 802.16 Commercial off the Shelf (COTS) Technologies as a complement to Objective Maneuver (STOM) Communications" September 2004. If more information is required concerning the specific parameters of 802.16, this thesis will cover all the networking specifics while this thesis will focus on modular topology implementations.

[117] The actual title for the IEE standard is "Air Interface for Fixed Broadband Wireless Access Systems"

and operations as an alternate to cable and Digital Subscriber lines (DSL)[118]. The IEEE 802.16 standard was approved on December 6, 2001, and provides the standard to frequencies between the 10 and 66 GHz range. The IEEE 802.16a standard was approved on April 9, 2002, the standard establishes "first mile/last mile" standards for connecting metropolitan broadband wireless, and is focused in the 2-11 GHz range.

WiFi (wireless fidelity – IEEE 802.11) has a much smaller footprint[119], an unstable media access algorithm and has difficulty propagating in metropolitan areas, IEEE 802.16 is an ideal much choice for establishing links between the wireless clouds established for client access[120]. Since IEEE 802.16 networks support up to 50 Mbps, and allow for the simultaneous transfer of data, voice, and video, sustained data rates of almost .5 to 2 Mbps can be provided to multiple users[121]. IEEE 802.11 components will still be used for client connectivity in this thesis, due to the limited number of client IEEE 802.16 technology on the COTS market today. Long-term focus will be on the total IEEE 802.16 M-FLAK package.

The IEEE 802.16 standard specifies a Media Access Control (MAC) layer designed for the support of multiple Physical Layers (PHY) in order to operate in many environments. The robust bandwidth of IEEE 802.16 enables thousands of DSL-size subscribers to be maintained on the MAC. IEEE 802.16 was designed to operate with both point to point (PtP) and point to multi-point (PtMP) network topologies.

The IEEE 802.16 also standards provide:

- Long range connectivity up to 30 miles
- Non Line of sight (NLOS) performance
- Multi-path operations
- Scalability

---

[118] http://grouper.ieee.org/groups/802/16/pub/backgrounder.html - Broadband Wireless Access: An Introduction to the Technology Behind the IEEE 802.16 WirelessMAN™ Standard. Other models for the application of 802.16 include an architecture which links the Radio-WAN directly into the client hardware.

[119] A few hundred meters depending on commercial access point and industry standard utilized

[120] 802.11 also have limited security capabilities and operates primarily on Carrier Sense Multiple Access – Collision Avoidance (CSMA/CA), which does not enable a scalable increase to larger numbers of users. Only later revisions of the 802.11 standards (802.11a and 802.11g) added the OFDM capability to its standards.

[121] Downloaded from Epicon

- Quality of Service (QoS) support to voice and video applications
- Routable networks within the 802 framework
- Multicast traffic support

The NLOS capabilities are due to the orthogonal frequency division multiplexing (OFDM) functionality of the IEEE 802.16 standards[122]. OFDM is described as

> a spread spectrum technique that distributes the data over a large number of carriers that are spaced apart at precise frequencies. This spacing provides the orthogonality in this technique which prevents the demodulators from seeing frequencies other than their own. The benefits of OFDM are high spectral frequency, resiliency to RF interference, and lower multi-path distortion[123].

IEEE 802.16 is also commonly referred to as WiMAX, the Worldwide Operability for Microwave Access. WiMAX is actually a business organization which has adopted various certifications within the IEEE 802.16 business community. WiMAX currently serves hotspots and wireless local area networks all over the globe. Current WiMAX companies include Motorola, Redline Communications, Intel, Fujitsu, and AT & T, ever-expanding the COTS research, and therefore products, which can integrated in a cost-effective manner[124]. Considerable research has been undertaken by all of these companies in the expansion of this technology standard to the mobile user.

2. Military Applications of IEEE 802.16

IEEE 802.16 standards have been growing in popularity among military operators for deployable applications. Currently, IEEE 802.16 topologies have been deployed to Iraq, the Horn of Africa, and Afghanistan in order to support networking insufficiencies in deployed combat units. The IEEE 802.16 equipment has been deployed to future applications of JTRS radios and represents yet another potential area for the adoption of IEEE 802.16 standards[125].

---

[122] http://www.standards.**ieee**.org/get**ieee**802/**802.16**.html

[123] OFDM Tutorial http://www.wave-report.com/tutorials/OFDM.htm Last downloaded on May 26, 2006

[124] www.wimaxforum.org – there are currently over 200 companies in the WiMAX Forum

[125] Downloaded from Epicon

JTRS utilizes a software-defined radio (SDR), which uses software for the demodulation and modulation of radio signals. JTRS is planned for integration into the GIG, will reduce the number of traditional radios in the field from 750,000 to 250,000, and shift with the concept of true NCW for the military, it is not built to upgrade with the acceleration of technology[126]. JTRS is not a modular system like IEEE 802.16 topology networks, and therefore is not easily upgradeable[127]. The expansion of JTRS from its current topology will include extensive integration, and require millions of dollars in software programming and architecture restructuring.

There are considerable obstacles to be overcome before JTRS can be fully deployed to operators in the field to fulfill all of the necessary requirements of a functional and secure MANET. This is an especially true in an expanding mission area such as the maritime security and riverine environments.

IEEE 802.16 equipment has been deployed to various theaters in the GWOT. Iraq and Afghanistan both have US Army and Marine Corps communications suites being operated for numerous missions in these combat theatres. This has been to handle the step of Division to Brigade, as well as Brigade to Company communications links. Unfortunately, the extension of these technologies has not been re-distributed to the disadvantaged operator across the digital divide. This precedence, and the success of the equipment in the field, firmly establishes the functionality of these technologies in adverse conditions. With further expansion of these technologies, the success of the scalability of these network architectures would be unprecedented.

3. IEEE 802.16e

IEEE 802.16e, also known as mobile WiMAX, was adopted as a standard by the IEEE on December 2005. The main capability of the IEEE 802.16e standard will be the "meshing capability" which will connect Base Stations (BS) and Subscriber Stations (SS) together through layer 2 protocols. This will enable the mesh capabilities of certain 802.11 WiFi networking gear to be applied to the IEEE 802.16 standard.

---

126 Munoz, p. 14

127 www.globalsecurity.org/JTRS/

By improving on facets of fixed position IEEE 802.16 standards from OFDM to OFDMA, a multi-user expansion of the protocol, the ability of mobile users to maintain connectivity will be greatly improved[128]. A new expansion of the OFDM-256 protocol used by fixed position IEEE 802.16 technologies is planned also, known as SOFDMA, or Scalable Orthogonal Frequency Divisional Multiplexing Access.

SOFDMA will improve upon OFDM256 for NLOS applications by:

- Improving NLOS coverage by utilizing advanced antenna diversity schemes, and hybrid-Automatic Retransmission Request (HARQ)
- Increasing system gain by use of denser sub-channelization, thereby improving indoor penetration
- Introducing high-performance coding techniques such as Turbo Coding and Low-Density Parity Check (LDPC), enhancing security and NLOS performance
- Introducing downlink sub-channelization, allowing administrators to trade coverage for capacity or vice versa
- Improving coverage by introducing Adaptive Antenna Systems (AAS) and Multiple Input Multiple Output (MIMO) technology
- Eliminating channel bandwidth dependencies on sub-carrier spacing, allowing for equal performance under any RF channel spacing (1.25-14 MHz)
- Enhanced Fast Fourier Transform (FFT) algorithm can tolerate larger delay spreads, increasing resistance to multi-path interference

New technological components are planned for release in 2006, and SOFDMA is the planned software application to enhance IEEE 802.16e capabilities. Unfortunately, SOFDMA is not compatible with OFDM-256. Still, current manufacturers of OFDM-256 are currently planning migration paths in order to compensate for this transition.

This adaptation will enable current network topologies which include IEEE 802.16a to be easily upgraded to IEEE 802.16e standard technologies. Upgrades to network architecture would simply require the addition of new Radio-WAN modules as they passed established standards.

[128] www.wikipedia.org

D MARITIME NETWORK TOPOLOGIES FOR IEEE 802.16 ARCHITECTURES

The Quadrennial Defense Report, published in 2005, highlighted the importance of interoperable communications in maritime security today. It specifically stated:

- Architectural design solution for the mobile communications needs of multi-mission capable small boats
- Routable, secure, modular, interoperable system of communications which can be used by multi-language military, constabulatory, and rescue forces both abroad and domestically
- Interoperable communications with non-governmental support as a capability[129]

The following topologies will establish the multi-mission capabilities of the maritime FLAK as a C4ISR tool to counter asymmetric threats. These multiple missions will highlight the versatility of the M-FLAK in the required mission parameters. Each of these topologies is based on the MANET principles #1 and #2 as explained earlier.

1. VBSS Topology

This topology establishes numerous platform-centric M-FLAK suites, which could link to each other, or connect from remote tactical locations to strategic and operational command nodes via a SAT-COM link. Each one of these units will maintain the platform-centric LAN with end systems, while each link will be the Radio-WAN IEEE 802.16 connection which can then be routed through the overarching GIG-BE architecture.

[129] QDR

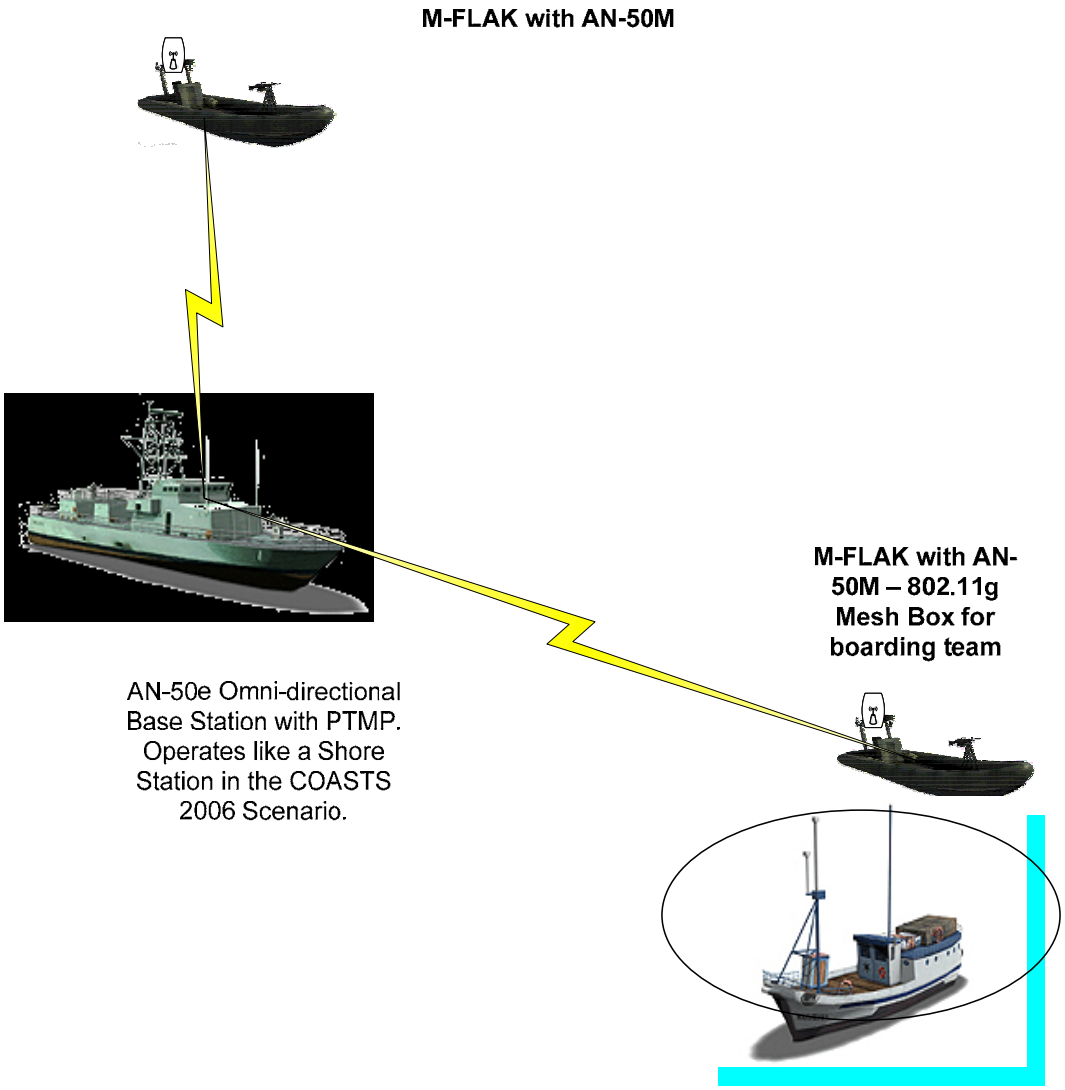

Figure 18. VBSS Network Topology for the M-FLAK

2. Riverine – Craft to Craft & Craft to Shore (Vehicle or Choke Point Security)

The following topology will build on the arguments formulated in the previous section, but will add another routable connection through a SAT-COM link. This will enable the remote riverine operator to maintain connectivity despite the extreme distances experienced by these operations. Because the C2 HUMVEE will maintain the same platform-centric LAN, the overall Radio-WAN links will be the same as the boat-to-shore and boat-to-boat connections.

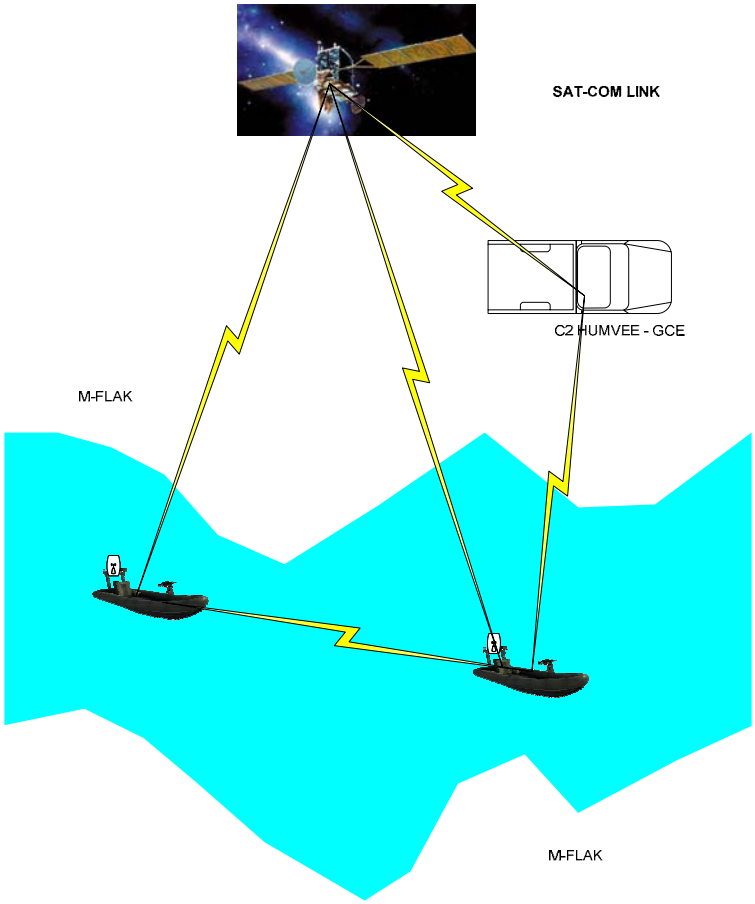

Figure 19. Riverine M-FLAK Topology

3. Harbor & Port Security

The harbor security topology reflects the easiest to implement since the distances required will be much less than the Riverine and Open Sea VBSS topologies. Also, the power levels on the shore arrays are easier to maintain. The same VBSS connectivity will be able to be maintained as ships are interdicted.

The harbor security topology matches the existing geography of the USCG UHF-FM high site system, which uses analog voice. This system provides port and coastal communications throughout the US. Essentially, an IEEE 802.16 Radio-Wan technology could be established using pre-existing real estate and hotel services.

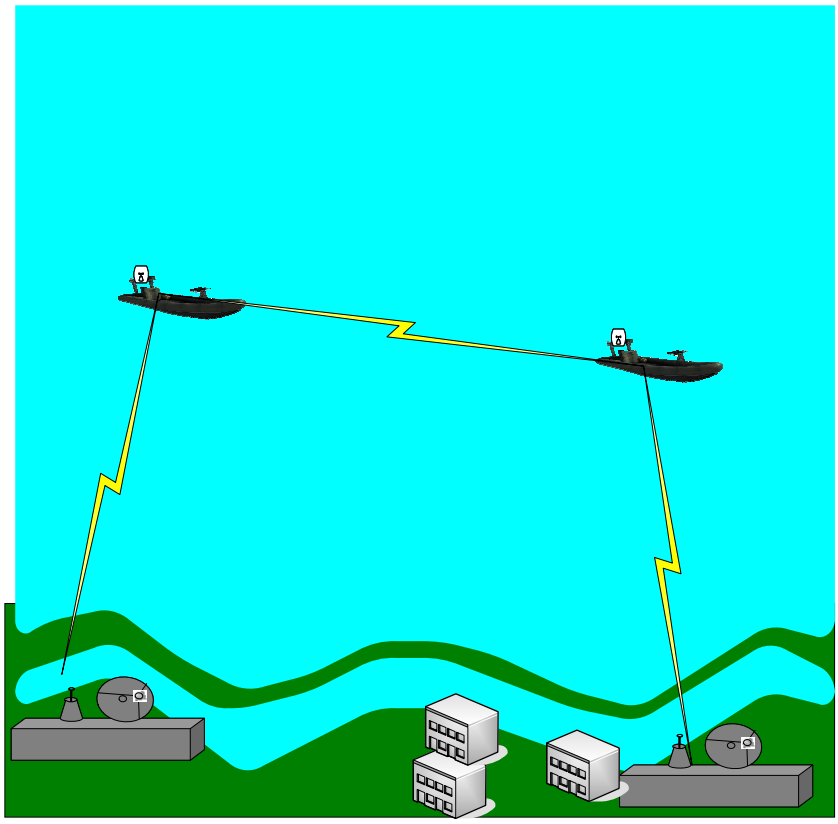

Figure 20. Harbor Security Topology

IV. MARITIME FLY AWAY KIT TECHNOLOGY

A. M-FLAK TOPOLOGY

The basic architecture for the M-FLAK will be based on the same concepts as the MANET requirements for effectiveness. It will be modular, scalable, interoperable, secure and manageable end-to-end. The technology below will be explained in two sections. The first are the networking components which function within the MANET architecture as explained in the last chapter. The second are the end systems which are utilized as components to the platform-centric principle #1 connections.

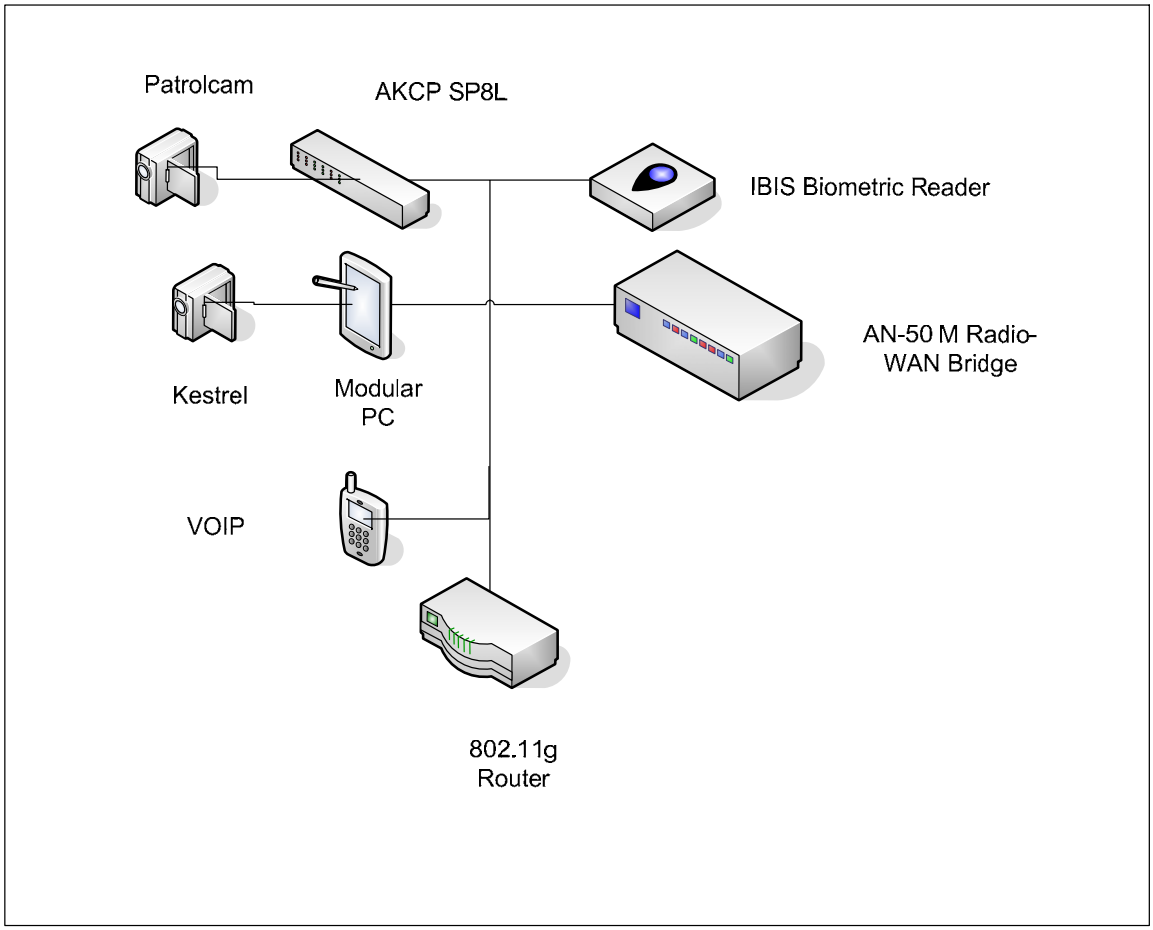

Figure 21. M-FLAK component technology – IS Principle #1 Architecture

Figure 21 contains the M-FLAK components which will be placed on the small boat. The Kestrel camera and Patrolcam are linked into the architecture using technologies which convert their signal[130] into a networked signal which can be transferred over the LAN and WAN. For this reason, their position is not the same as the other end systems.

Figure 22 establishes the link between the multiple LANs around the globe, which can then send, receive, and view data from the various end systems operated by the remote users.

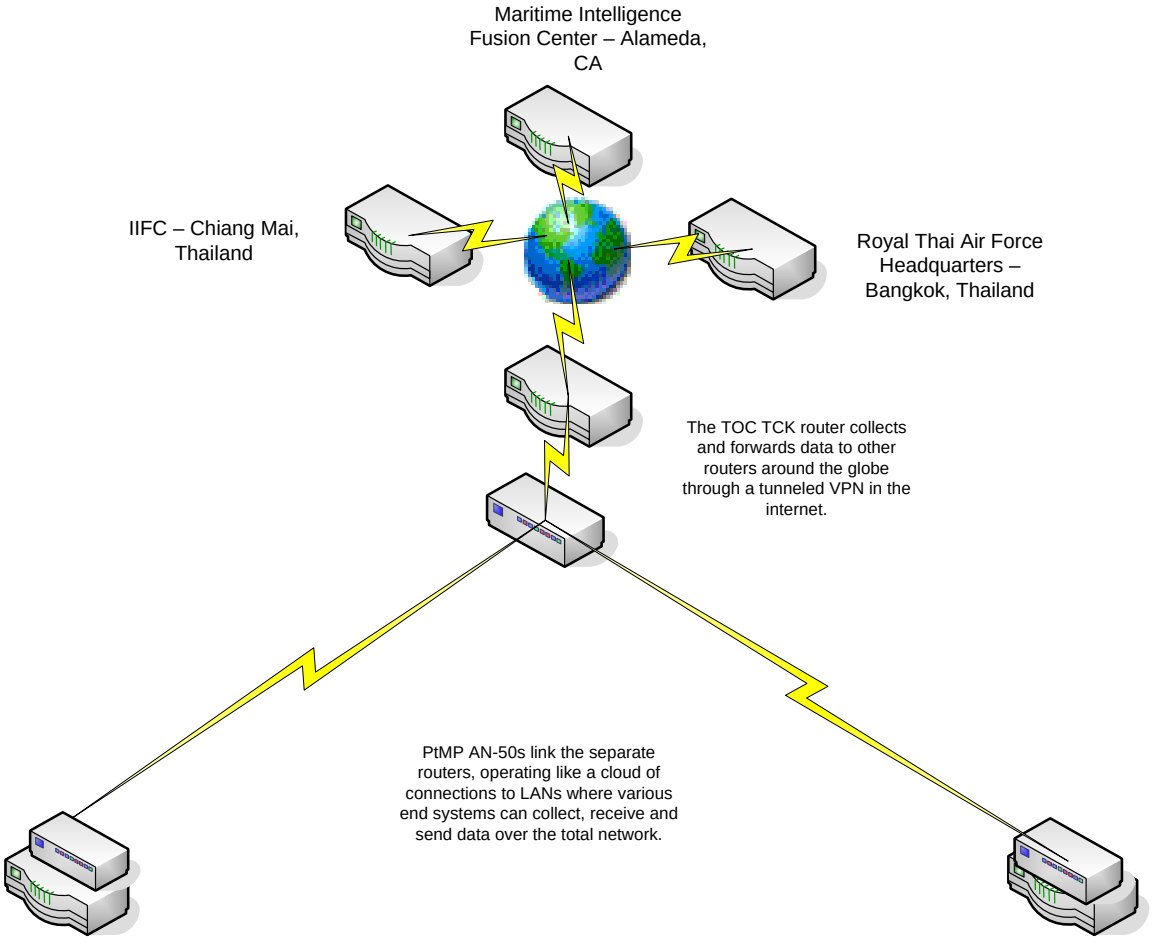

Figure 22. M-FLAK Network Topology – Information System #2 Architecture

[130] Analog signal in the case of the Patrolcam and Digital, but not IP, in with the Kestrel Camera.

1. Network Components

a. Redline AN-50e Communications Bridge

The "Master" station to be used in the maritime network topology is the Redline Communications AN-50e Point-to-Multi-point (PtMP) Base Station (BS). As a Point-to-point wireless communications suite, the AN-50 is capable of passing NLOS broadband signals at 54 Mbps at a distance of 30 kilometers (km). In PtMP mode, the BS is able to pass as much as 35 Mbps over distances of 15km.

Two different configurations are planned for the shore based antenna array. One entails an AN-50e in a PtMP mode. The second configuration entails one AN-50e for each antenna in the array. Both were tested, and both showed various advantages. Most of the considerations for implementations will revolve around the costs associated with the different topologies.

Figure 23. AN-50e Wireless Base Station

b. Redline AN-50M Communications Bridge

The AN-50M is the man-portable version of the AN-50e wireless networking bridge. The AN-50M will be used in the maritime FLAK as the mobile bridge. Depending on range, using the PtMP mode, bandwidth has been passed as high as 35 Mbps with the higher-level firmware software additions. On the standard firmware levels, 15 Mbps is passed from unit to multiple units.

Figure 24. AN-50M Wireless Base Station

c. Hyperlink Sectored 360 degree Omni-array

The 5.8 GHz omni-directional sector antenna arrays include four 17 dBi, 90 degree, sectored antennas produced by Hyperlink Technologies, Inc.

Figure 25. Hypergain HG5817P-090 Wifi antenna array

Each sector antenna is a Hypergain HG5817P-090 WI-FI antenna. Each sectored antenna produces an eight degree vertical beam width up to 100 Watts in

conjunction with the 90 degree horizontal beam width. A four-way splitter connects the four antennas together to the AN-50e bridges. The RF pattern resulting from this antenna configuration is as follows:

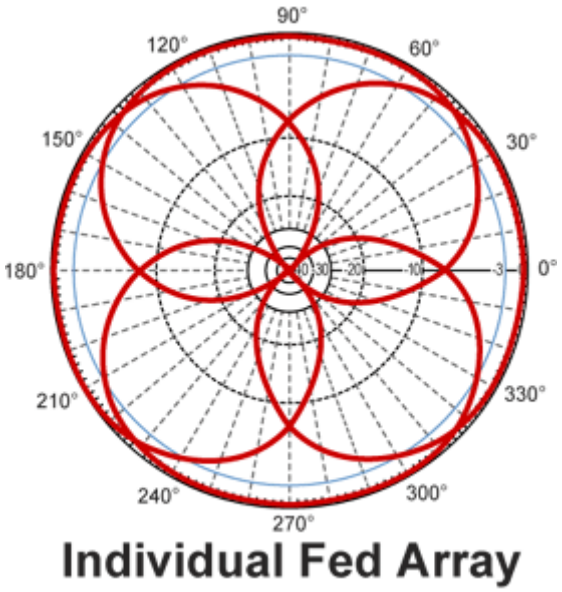

Figure 26. RF Propagation form the Sectored Omni Array

Each sector antennas of the individually-fed array will have RF propagation as follows:

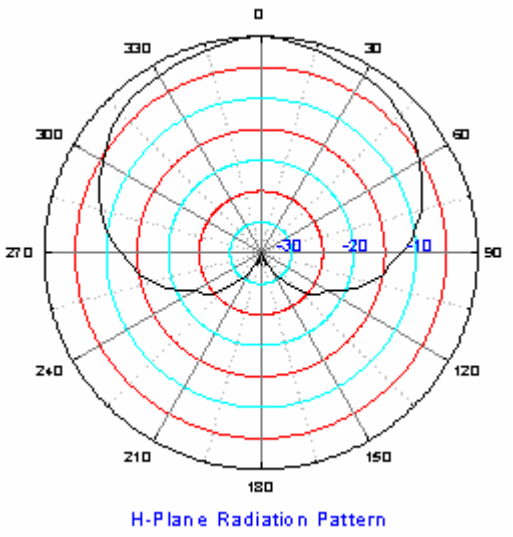

Figure 27. RF Propagation from the Sectored antenna

The horizontal beam-width of the antennas, which combines four 90 degree sectors into a full omni-directional array, is balanced with a nine degree vertical beam-width. This requires the shore antenna arrays and the sea-based antenna arrays to be placed at comparable heights.

In order to test alternate antenna configurations, a 5.8 GHz antenna array using four 13 dBi, 90 degree sector antennas, with a smaller "sail-area" to compensate for configuration ergonomics, was utilized in the March 2006 NPS COASTS field experiment in Thailand.

Figure 28. Superpass 13 dbi antenna

d. D-Link Commercial Ethernet Switch

Switch: In order to increase the client technology available to the modular kit, an eight-port switch to connect the Modular PC, ACK box, and the IEEE 802.11g wireless access point to the IEEE 802.16 AN-50M base station in the M-FLAK. Also, other client technologies can be directly linked into the Switch.

Figure 29. D-link four-port Ethernet Switch

e. AKCP Sensor Probe Eight Linux (SP8L)

AKCP Sensor Probe 8 Linux (SP8L): The AKCP Sensor Probe 8 Linux "black box" is a Linux programmed network tool which enables non-IP sensors to be linked into a TCP/IP protocol network. This capability will be vital for coalition allies who have invested in other proprietary security network technologies because it enables these technologies to be integrated into the full network, assigning them IP addresses in its Linux server. Even traditional stereo AV cable-fed sensor inputs will be able to be viewed across the network architecture, no matter the distance.

The addition of the AKCP box enables the proprietary equipment utilized in the M-FLAK to become "good citizen" technology[131]. This means they are able to talk to other network gear on the principle #1 LAN. Even more important, they are routable to other platforms. Like the second principle in the MANET requirements, this enables the transfer of packetized data throughout the devised networks.

[131] Buddenberg, Good Citizen Technology

Figure 30. AKCP SP8L Box – Front View

For the maritime FLAK, the SP8L, a standard rack-mounted black box was placed in the roto-roll SKB cases along with the AN-50M. The rear opening of the SKB case enabled any non-traditional sensor cables to be easily linked into the box.

Figure 31. AKCP SP8L Box – Back View

The SP8L has eight RJ-45 configurable sensor ports, can work with any type of current operating systems, a 32-bit ARM processor, 64 MB of SDRAM, and 128 Megabytes of volatile FLASH memory. The SP8L can connect up to four cameras, which means two cameras can be added to the current topology.

The SP8L utilizes SNMP, an important requirement for end-to-end management. The important factor to understand here is that the AKCP box is one of the components which turns peripheral technologies into the proverbial "good citizens".

2. M- FLAK End Systems

According to the requirements of an establishing a MANET:

> The apex of information systems architecture is the interface that defines how end systems (the sense, decide and act modules) attach to the supporting internet-work. End systems can be easily attached to an internet … providing that these end systems qualify as Good Network Citizens.[132]

This means that any end system attached to a LAN, as defined by the Information System requirement in principle #1, must be able to transmit data through the network and over the combined network topology. This concept entails the idea that even a toaster can be connected to the internet as long as it has the capability to speak to other components through Layer 3 protocols.

Many of the following technologies added to the M-FLAK are not "good citizens," but can be made good citizens through the addition of the AKCP SP8L box.

a. Kestrel-Tech wearable USB Camera

Kestrel wearable USB powered camera: Attached to the Modular PC, which enables the dual role of a functional computer for the small boat operator, as well as a portable, wearable, and ergonomic computer for members of the boarding team. Using a shoulder-mounted tripod, the camera will enable any operator on the Shared

[132] Buddenburg, p. 1, "Of Good Network Citizens and Internet Toasters." Feb 2000

Situational Awareness (SSA) application to view and control the camera's view. In the current testing topology, the Kestrel camera will be fed through the network by a web-server application[133].

Figure 32. Kestrel-Tech USB Powered Camera worn by LT Hochstedler in Thailand

b. Modular Computing Company's (MCC) Modular PC

Modular PC Computer: The computer system utilized in the M-FLAK is the Modular PC system designed and created by the Modular Computer Corporation (MCC). The Modular PC is a ruggedized computer which can be shifted from various input and output housing modules. This makes the Modular PC ideal for tactical situations since it can be used in different modules depending on the mission while still maintaining powerful processing speed.

[133] The Software video application used for this testing was Webcam XP

Modular PC specifications:

- 30 GB Hard Drive
- 1 GHz Processor
- Windows XP
- 512 MB RAM
- 6.3 Display Screen (Daylight Readable Screen)
- Extended Long-life battery to 5.5 hours
- Fold-able keyboard

Figure 33. Modular PC

c. Patrolcam

Patrolcam: The primary camera to be utilized in the FLAK is the Patrolcam. The Patrolcam is a heavy-duty, outdoor, security camera designed for mobile units. Originally designed for Police, SWAT, fire, and inspection vehicles in the United States, the camera has a nitrogen-encased lens to prevent fogging, a solid aluminum casing for survivability, and image stabilization to maintain an anti-jitter video feeds during erratic motion. These features make it the ideal camera for the rough water movement of small boats across water.

The camera also possesses a Near Infrared capability, making the unit functional as an ISR tool in the day as well as the night. Since the Patrolcam is a proprietary technology, and not an IP camera, the Patrolcam will be linked via an AKCP video processor, which links the video feed from the camera to any location on the network.

Camera Specifications:

- 25X Optical / 12X Digital Zoom
- 5.5” Readout screen
- Standardized Thule Roof Rack

Figure 34. Patrolcam and Proprietary joystick

3. Miscellaneous M-FLAK Equipment

a. SKB Roll-Shock Case

SKB Case: In the construction of the M-FLAK, a roll shock case produced by SKB cases was used. SKB Inc. produces military standard (MIL-STD) cases for multiple applications. A 6-rack deep roll-shock was chosen for the FLAK design because all necessary electronics equipment can be hard-mounted within the case. Also, the vehicle mounts for the Modular PC can be affixed to the cases with extreme ease.

Figure 35. SKB Roll Shock Case 6R

b. Power

The UB 2590 Battery is the current power source for the AN-50M bridge. Two batteries power each AN-50M for almost seven hours of continuous operations.

Figure 36. UB2590 And 12 volt batteries

Also, in order to power the Switch, Patrolcam, and ACK, twelve volt automobile batteries, and a DC to AC inverter, were used to maintain power. These batteries powered the switch, SP8L, and the Patrolcam. The shore arrays and AN-50e were powered by AC power in the Tactical Operations Center (TOC) - this is the physical location where all other aspects of the network, to include the various MANET requirements established in the previous chapter, are connected into an interoperable SSA for watch-stander use..

4. Miscellaneous Network Equipment

Miscellaneous Network Equipment contributed by the Coalition Operating Area Surveillance and Targeting System (COASTS) research project. Various cables were used to connect the maritime FLAK components: ethernet cables, cross-over cables, and input components. Also, certain software and networking applications contributed to the testing of the M-FLAK. These technologies are examples of the NCA applications which will be employed by the various service-centric network architectures.

a. C3Trak Shared Situational Application (SSA)

C3Trak is a joint corporate/NPS student software SSA which fuses the collective data of the network sensors into a collaborative graphical user interface (GUI). C3Trak is designed to produce a graphical representation of all sensor data, over a 3D topographic representation much like Google Earth. Icons were placed in order to enable operators to “point and click” the 3D ICONS, and be able to produce video and data without a need for language translations. As a tool for further integrating the multi-language multi-nation coalition operations of the future, applications similar to C3Trak will be vital. These same types of applications will be necessary in order to break through the language barriers faced in constabulatory and military operations.

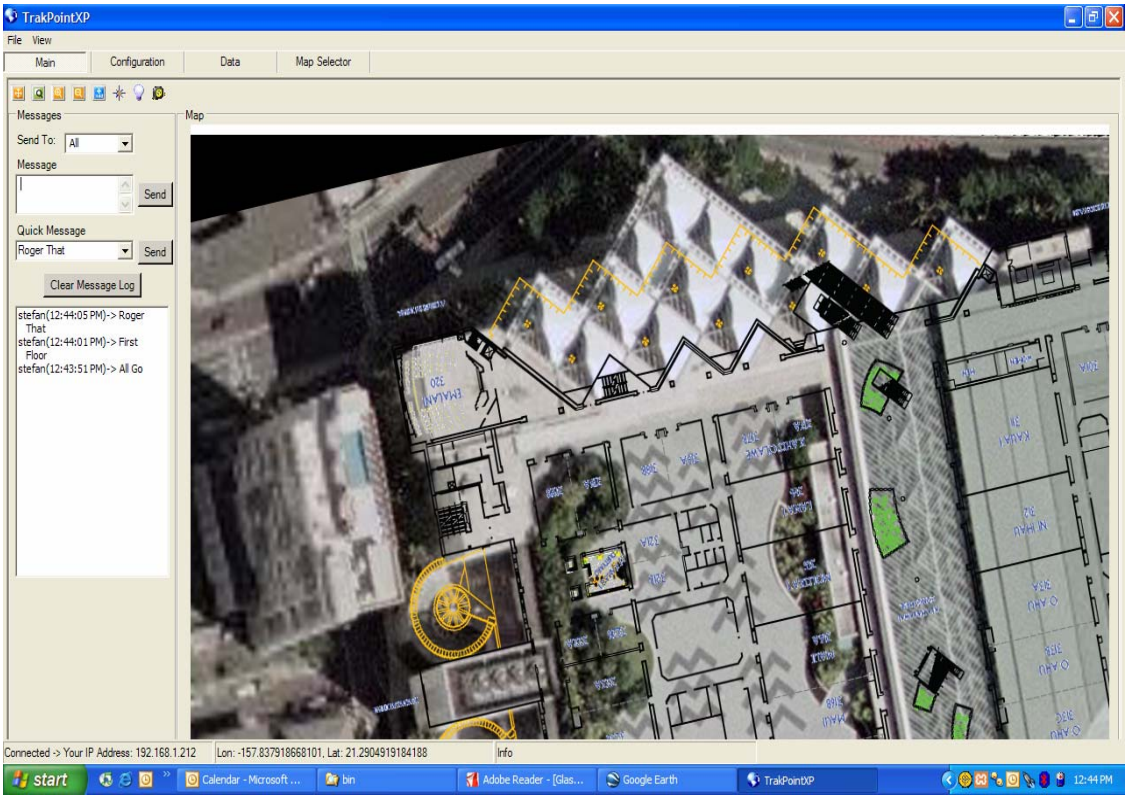

Figure 37. Shared Situation Awareness (SSA) applications C3 Track

b. 802.11g Mesh Dynamics Access Point

Figure 38. IEEE 802.11g Mesh Dynamics Wireless Access Point (AP)

The IEEE 802.11g wireless access point will establish connectivity from the small boat to the boarded ship. This will enable the utility of the Modular PC, the Kestrel

camera, as well as other associated biometric client applications to extend beyond the maritime craft to other vessels. This radio will operate in the 2.4 GHz frequency range using a 400mWatt radio.

c. Identix Biometrics Handheld Unit

Figure 39. Identix Biometrics Reader

The Identix corporation biometric reader enabled fingerprints, photos, and biometric profile data to be recorded, and then sent, via the FLAK to the portable SAT-COM connections, and back to the various intelligence fusion centers for comparison. The IBIS reader takes photographs and fingerprints from suspects and transmits the data over a wireless connection to a remote, updateable database.

This database can be linked into larger biometrics databases, enabling the remote operator to update and reference larger levels of constabulatory data than before.

d. Air Force Battle Lab (AFBL) Explosive Material Device

The AFBL is currently conducting testing with a COTS explosive analysis device which works much like a breathalyzer does for drunken driving stops in the US. This device detects residue chemicals up to ten days after an individual has been exposed

to them. With the addition of this device to the M-FLAK, the detection of the users, creators, and transporters of improvised explosive devices (IED) can be extended to maritime forces around the globe. Although this modular and portable unit does not have the networking capability of the IBIS, it is a key way to supplement the biometrics data being collected by the operators at the remote tactical level.

Figure 40. AFBL Explosive Materials Detection Device

e. CISCO Tactical Communications Kit (TCK)

Figure 41. Tactical Communications Kit (TCK)

The CISCO Tactical Communications Kit (TCK) includes the following equipment:

- CISCO 2811 Router
- VOIP Call Manager
- AC/DC Power Inverter

For the purpose of the COASTS 2006 experiment, the TCK was used to show VoIP capabilities, a mobile routing system, and the modularity of total communications systems for multi-mission capabilities. Donated by CISCO for experimentation immediately after NPS's deployment of a Hastily Formed Network (HFN) to Hurricane Katrina relief efforts in coastal Mississippi, the TCK is built to overcome stove-piped communications capabilities among military, law enforcement, fire, and other first responders.

B. COMBINED M-FLAK

1. Small Boat

Once all of these components are integrated in the M-FLAK, the modular design for the "last mile" tactical operator is achieved. The reduced footprint is vital due to the need for this equipment to be commercial airline transportable, as well as reasonable to transport on smaller riverine craft.

Figure 42. M-FLAK on the Speedboat during the May 2006 COASTS deployment

2. Boarding Officer

The composite boarding portion of the kits will culminate in the wearable Modular PC and the Kestrel camera. The link between these modules and the M-FLAK on the boat will be maintained by a link over an IEEE 802.11g encrypted wireless connection. Using a COTS software application known as Webcam XP, the video feed is turned into an IP broadcast across the network much like the AKCP SP8L converts the proprietary feed from the Patrolcam to the network from the M-FLAK.

Figure 43. LT Hochstedler in the Boarding Officer gear using Kestrel Camera and Wearable Modular PC

V. LABORATORY AND FIELD EXPERIMENTATION

The field and laboratory experimentation for this thesis spans seven months. This experimentation focused on studying the weaknesses and strengths of the maritime FLAK, and its ability to fulfill the QDR requirements for distributed network architecture in coalition littoral and riverine environments.

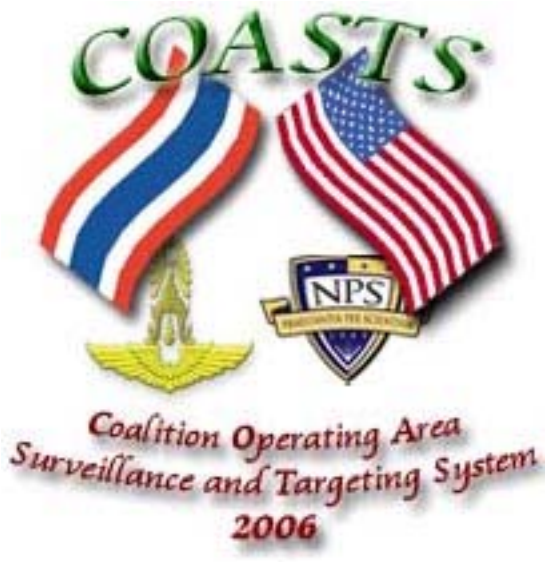

Figure 44. COASTS 2006 Logo

A. COALITION OPERATING AREA SURVEILLANCE AND TARGETING SYSTEM (COASTS) EXPERIMENTS

1. Background

The COASTS field experiment is an on-going research project based at the NPS. The COASTS field experimentation program supports U.S. Pacific Command (USPACOM), Joint Interagency Task Force West (JIATF-W), Joint U.S. Military Advisory Group Thailand (JUSMAGTHAI), U.S. Special Operations Command (USSOCOM), NPS, Royal Thai Armed Forces (RTARF), and the Thai Department of

Research & Development Office (DRDO) science and technology research requirements relating to theater and national security, counter-drug and law enforcement missions, and the Global War On Terror (GWOT)[134].

The COASTS program was designed to integrate the technological expertise of NPS's education and research resources with the science and technology (and potential operational requirements) of the Royal Thai Air Force (RTAF) using WLAN technologies to fuse and to display information from air and ground sensors to a real-time, multi-level, coalition enabled command and control center. Using COTS technologies, the COASTS research program intended to demonstrate the capacity of coalition communications in an operational context.

In 2005, the COASTS program completed a successful deployment of COTS NCW technologies in a tactical field deployment in Lop Buri, Thailand. The deployment included: integrated sensors, 802.11b WiFi, portable SAT-COM units, IEEE 802.16 PtP, UAVs, Deny GPS units, and SSA technologies. All of these were integrated into a system of systems for tactical deployment in a land-oriented counter-narcotic operational scenario. Based on the successful technologies from the 2005 deployments, an expanded 2006 deployment to the Mae Ngat Dam, 60 kilometers north of Chiang Mai, Thailand was implemented.

2. Network Architecture

The network that was designed for COASTS 2006 supported real-time video, integrated sensors, unmanned aerial vehicles, and situational awareness tools from 802.11 a/g mesh and IEEE 802.16 PtMP devices. The backbone link of IEEE 802.16 point-to-point suites was used to link the RTAF Wing 411 communications station to the Royal Thai Army (RTA) Inter-agency Intelligence Fusion Center (IIFC) and to the Mae Ngat Dam area of operations (AO).

At the Mae Ngat Dam AO, various sensors were integrated into this "system of systems" to create an "unblinking eye" of a tactical coalition C4ISR network architecture. In an IEEE 802.11g mesh WiFi cloud, various sensors and clients were integrated into the

[134] COASTS 2006 CONOPS

network. Ultra-wide band sensors, IP cameras, UAVs, as well as various client applications and hardware, were enabled through the network.

The COASTS' "last mile" technology linked through the IEEE 802.16a backbone to the RTAF Headquarters, the IIFC, and the SAT-COM communications capabilities from the Wing 411 communications station to the Maritime Intelligence Fusion Center (MIFC) in Alameda, CA. This last satellite link also established the ability of numerous global databases being linked through a virtual private network (VPN) to a distributed operator in the field, no matter how remote the location.

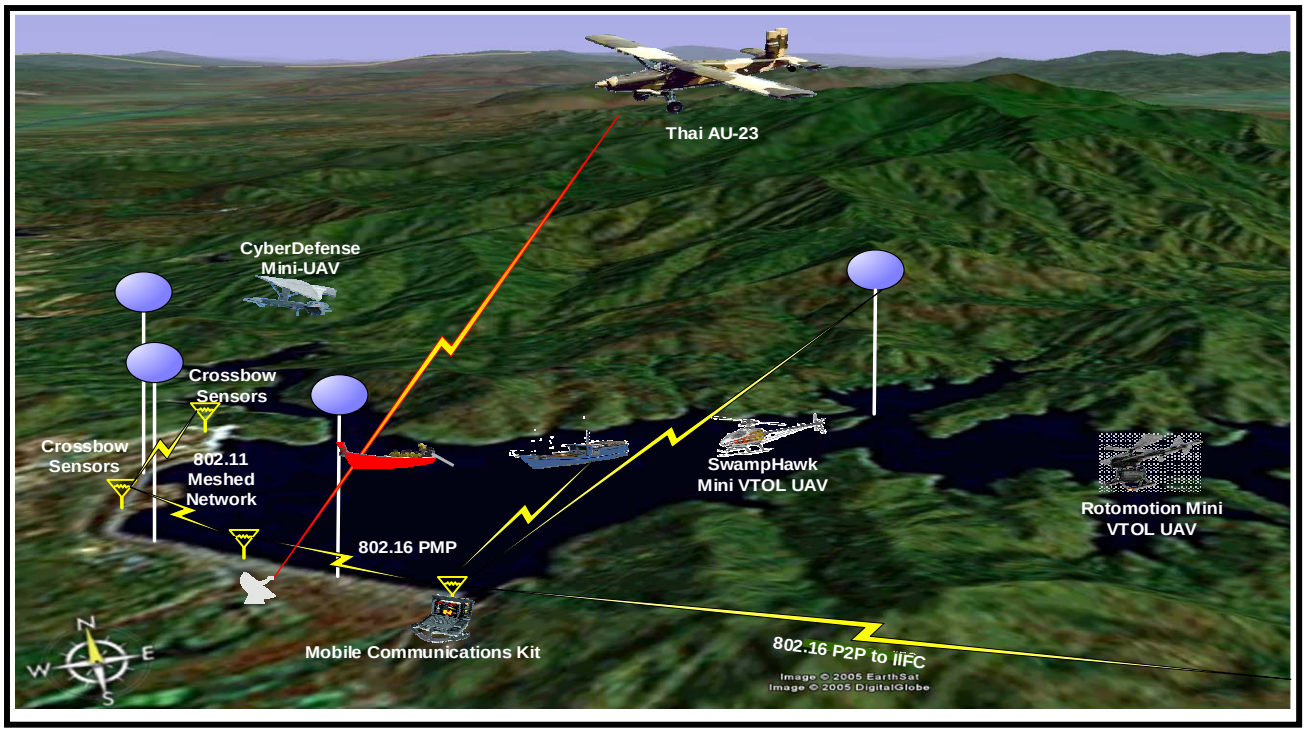

Figure 45. COASTS Mae Ngat Dam Operating Area (AO)

Figure 40 represents the COASTS 2006 network diagram as well as the IEEE 802.16a reach-back to the various intelligence fusion centers. The crucial elements of the network topology are as follows:

- IEEE 802.11 b Distributed Sequence Spread Spectrum (DSSS)
- IEEE 802.11a/g Orthogonal Frequency Division Multiplexing (OFDM)
- IEEE 802.16 OFDM (Stationary)
- IEEE 802.16 OFDM (Mobile)
- SATCOM
- Situational Awareness Overlay Software
- Wearable Computing Devices
- Air, Ground, and Water Integrated Sensors
- Mobile C2 Platforms
- Unmanned Aerial Vehicles (UAVs) (Fixed wing)
- UAVs (Rotary wing)
- Unmanned Multi-environment micro vehicles
- Ultra-wide Band Integrated Sensors
- Deny-GPS Inertial Gyro technology
- Network Security Applications
- Compression software applications
- Biometrics applications

Extending from the Mae Ngat Dam AO, a multi-hop IEEE 802.16a link connected the regional counter-narcotic IIFC in Chiang Mai city. Satellite links and VPN tunneling through the commercial internet provided a secure throughput to the global MIFC in Alameda, CA, as well as a regional “strategic” command center (simulated at the Naval Postgraduate School in Monterey, CA).

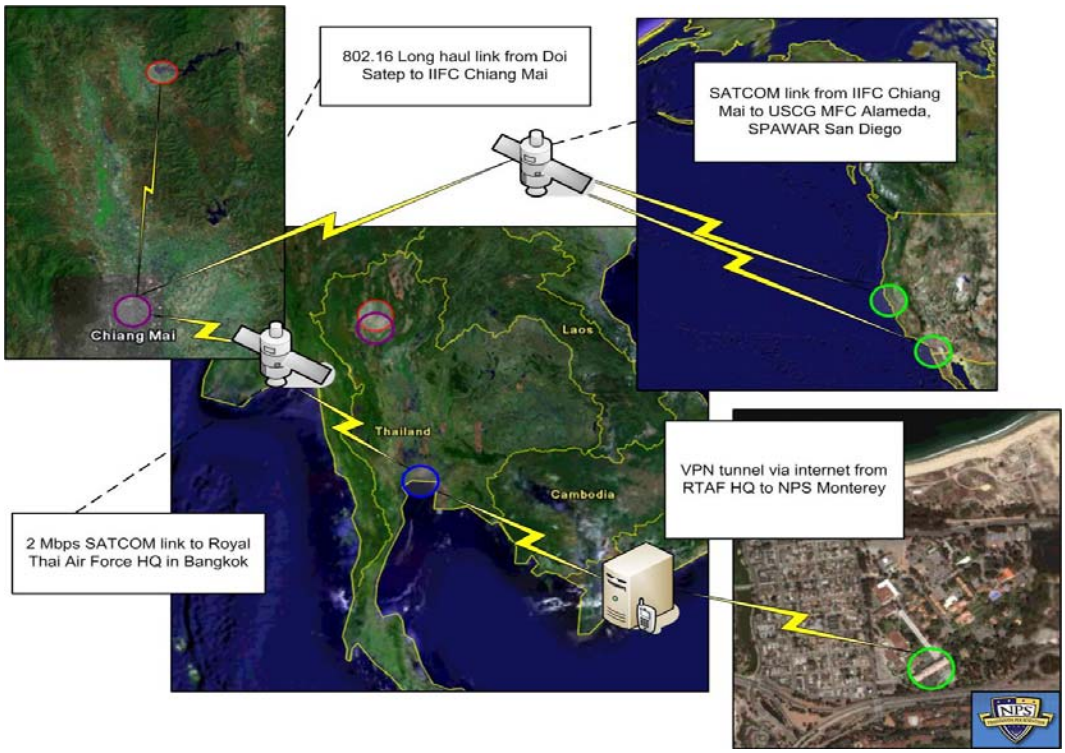

Figure 46. COASTS 2006 Global Network Topology

The breakdown of the overall COASTS 2006 network in a component diagram establishes the technological components used to establish the links across the geographic positions in Northern Thailand, as well as across the Pacific Ocean.

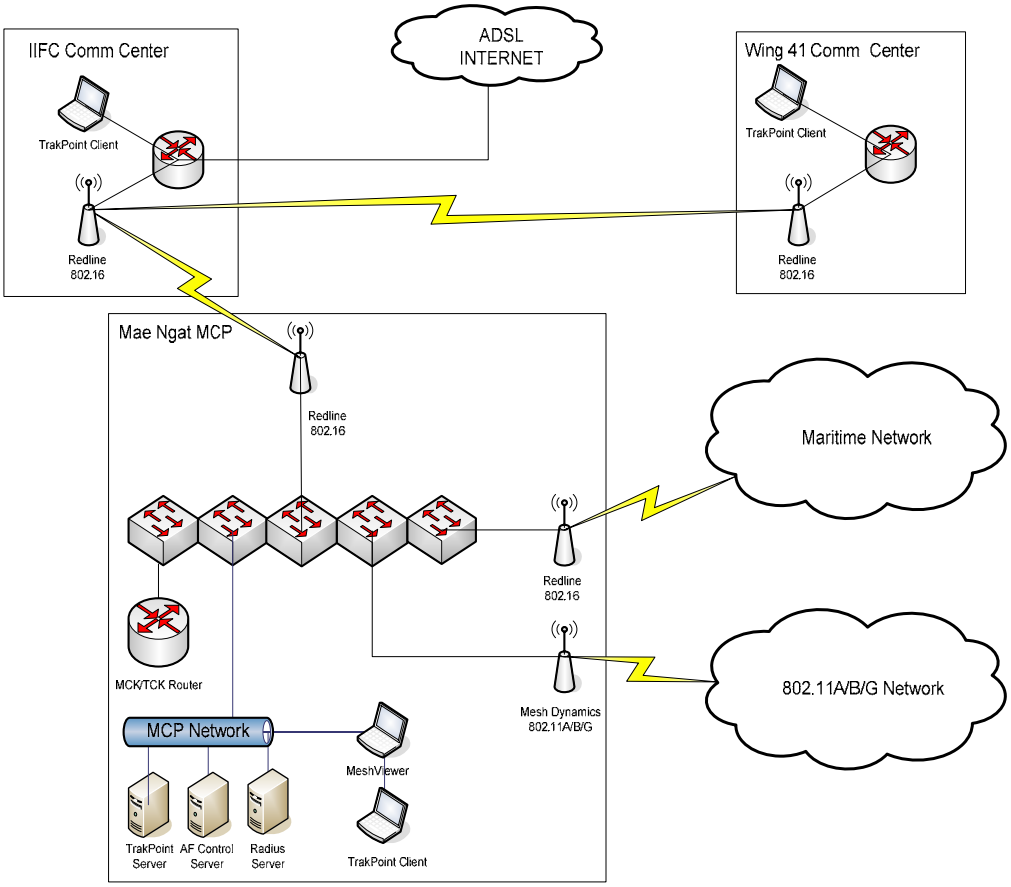

Figure 47. Overall Mae Ngat Dam Network Topology

The maritime component of the COASTS 2006 network topology is where the combined M-FLAK was evaluated. The COASTS 2006 scenario established the framework where the technological portions of the M-FLAK were field tested, as well as the numerous MOEs established earlier in this thesis.

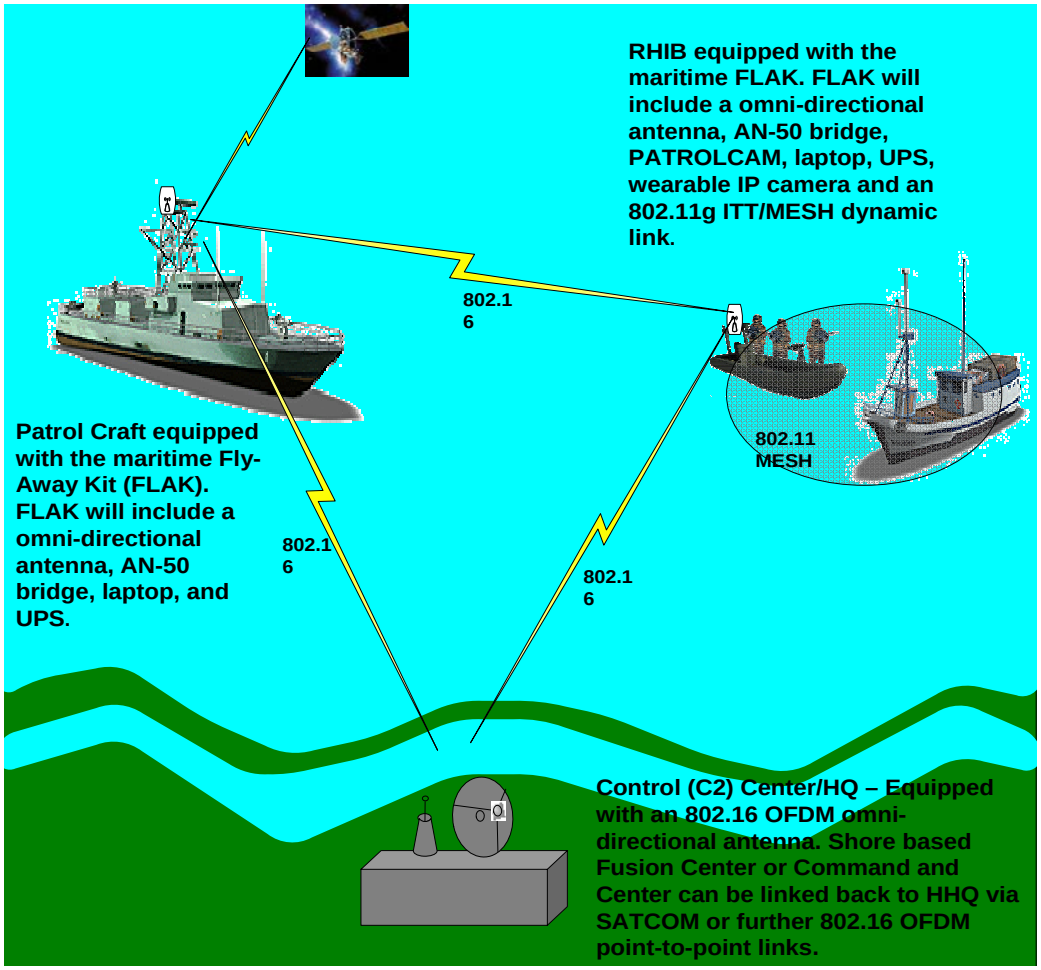

Figure 48. COASTS 2006 Maritime Network Topology

Although the maritime tests were a small portion of the overall COASTS 2006 network topology, it provided significant qualitative and quantitative measurements of the performance levels of the M-FLAK and its components.

3. Measures of Performance (MOP)

The COASTS exercise scenario provided an operational context in which to test the qualitative measurements of the capabilities of the maritime FLAK. The ability to maintain a solid persistent connection - while operating at speeds of 20 to 25 knots - was deemed the most significant gauge of performance. The separate components in the M-FLAK were studied concerning their own levels of performance.

The Kestrel camera and the Patrolcam were measured by their ability to transfer real-time video feeds to the Tactical Operations Center (TOC). The speed of the packets

to be transferred from the TOC to the Monterey MIFC was also evaluated. The Patrolcam was analyzed individually concerning its ability to send anti-jitter video feeds while moving at high speeds. The tests of the Patrolcam also relied heavily upon the performance of the AKCP SP8L boxes.

The ability of the SP8L to convert analog signals into digital TCP/IP packetized data was the deciding factor in whether the Patrolcam could remain as an integrated portion of the M-FLAK. Since the Patrolcam is a proprietary technology without a TCP/IP capability, this prevents the camera from being fully integrated into a networked system. The success of the SP8L will establish whether non-digital technologies can remain as a portion of coalition inventories working with modern network-centric US forces.

Other component technologies have been tested in various commercial and military applications, so exact performance measures are not necessary. The performance of these components will be analyzed in the context of the overall performance relative to the M-FLAK[135].

4. Measure of Effectiveness (MOE)

These measures are quantitative, and demonstrate mathematical value for the research questions proposed in the thesis introduction. Two separate software applications: RF Monitor and IX Chariot were used to analyze the performance of the M-FLAK in the 80216 network topology.

RF Monitor performed a dB measurement of the RF signal from AN-50 radio bridge to bridge. The dB measurements taken by the RF monitor can be used to establish the distance the links are capable of reaching, as well the survivability of the links in adverse conditions such as climate changes, as well as the effects of kinematics upon the performance of the link.

IX Chariot is a network management tool, which measures bandwidth between network link access points and bridges. IX Chariot, much like RF monitor, enabled a

[135] Kestrel Camera, Switch, Patrolcam, and VOIP phones.

numerical measurement of the bandwidth maintained by the IEEE 802.16 links. All of the results from these tests were integrated in chart form to establish performance parameters of the equipment.

5. Pre-Deployment Exercises (December 2006)

The initial M-FLAK tests involved only one IEEE 802.16 AN-50M mobile box and a PtMP AN-50e base station. These tests occurred at Pt Sur and were originally intended to be conducted using USCG boats off of the coast of Pt Sur in California. Unfortunately for planning and testing purposes, equipment was not available until the after commencement of the trials, and the over-water portion of the tests had to be canceled.

A reduced proof of concept was conducted using an AN-50e PtMP unit and an AN-50M placed on a 4X4 Jeep Cherokee. Short range runs were devised over the limited driving area in order to establish a baseline of RF parameters under different speed conditions. Since there was a much reduced ability to drive over the terrain at the Pt Sur station, the test was limited to less than a quarter mile distance. Also, the elevation of the region prevented long directional tests on the equipment. These were scheduled for future iterations in January and February of the following year.

Figure 49. USN SOSUS Station Pt Sur, CA Sonar Station

The collective tests resulted in a steady short range PtMP link which base-lined at 35Mbps in straightaway driving and 16Mbps during erratic and evasion driving. These results were kept as laboratory proof of concepts.

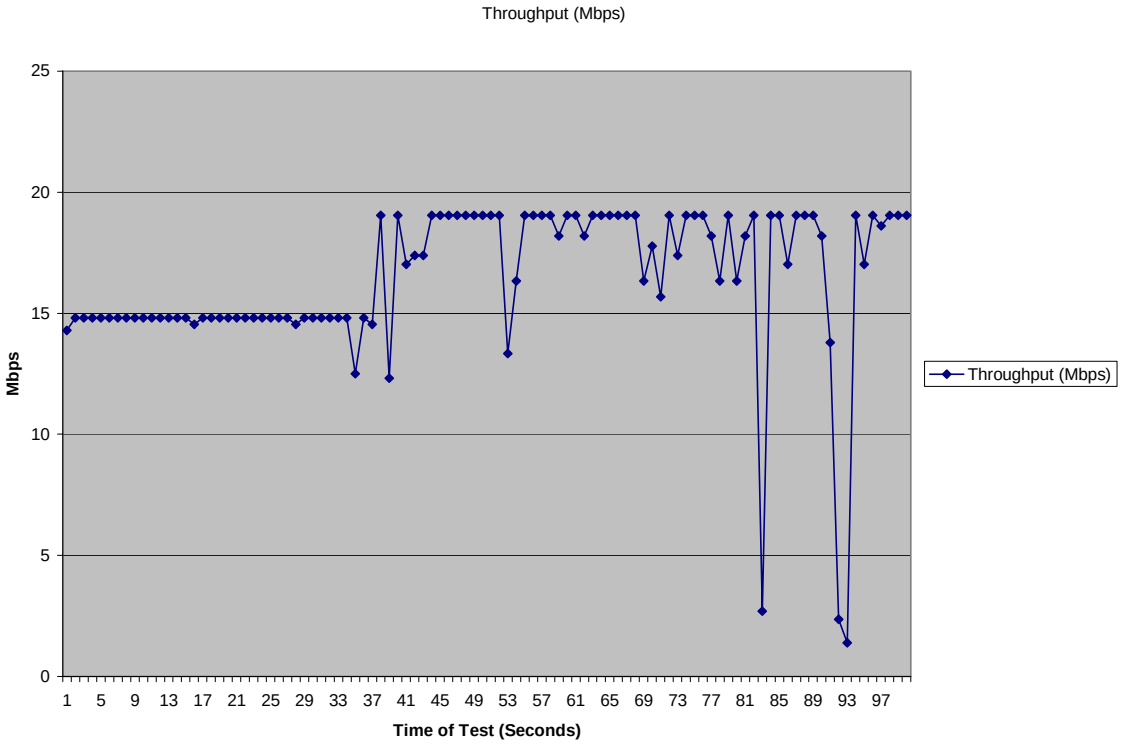

Table 1. Point Sur PtMP IX Chariot throughput tests (straightaway driving)

In Table 1, the performance measurements reflect a 16 Mbps level of throughput during erratic driving[136]. The increase to an 18 Mbps average occurred when the profile of the driving shifted to a different vehicle profile with fewer blockages from the frame of the Jeep Cherokee's luggage racks. This affirms the need for proper antenna placement when dealing with a mobile vehicle. Considerations for whip antennas or electronically steer-able antenna (ESA), both of which could operate above the vehicle superstructure, are planned for future testing iterations as resources permit.

After the straightway trials were conducted, erratic driving patterns were executed in order to measure the ability of the link to be maintained while pursuit patterns were being executed. 360 spins, high accelerations, quick decelerations, and zig-zag patterns were driven over off-road terrain in order to test the link throughput loosely simulating

[136] Zig-zag patterns as well as full 360 and 180 turns

pursuit and interdiction maneuvers of a small boat. The off-road terrain enabled enough up and down movement on the Jeep to simulate a typical littoral sea state.

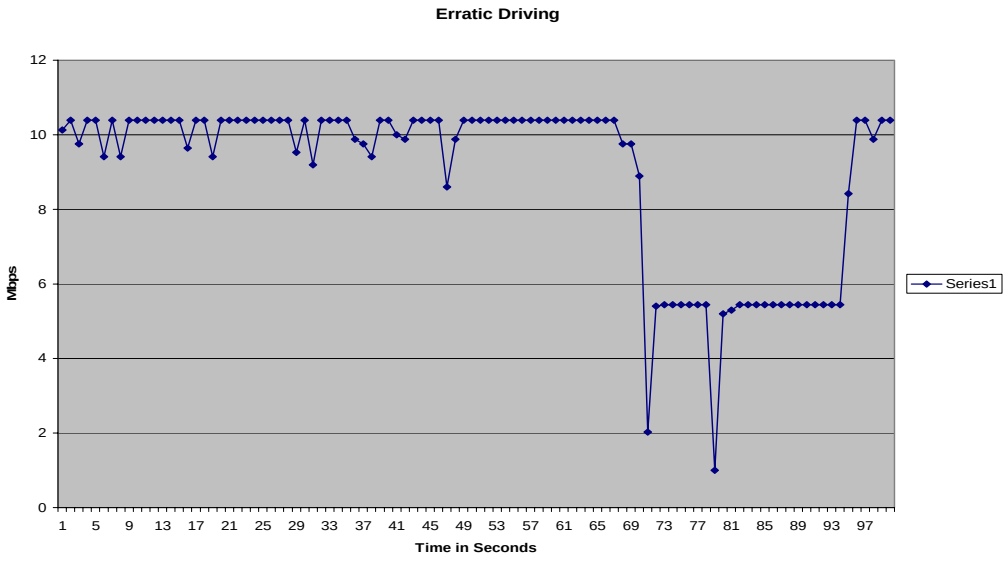

Table 2. PT Sur Erratic Driving IX Chariot results

Although there was a significant decrease in throughput detected be IX Chariot when severe turns and driving patterns were enacted, these decreases were not enough to sever the link between the AN-50e at a fixed operations center and the AN-50M placed in the Jeep. The most significant degradation occurred during turns which blocked the mobile antenna from a LOS connection to the operations center.

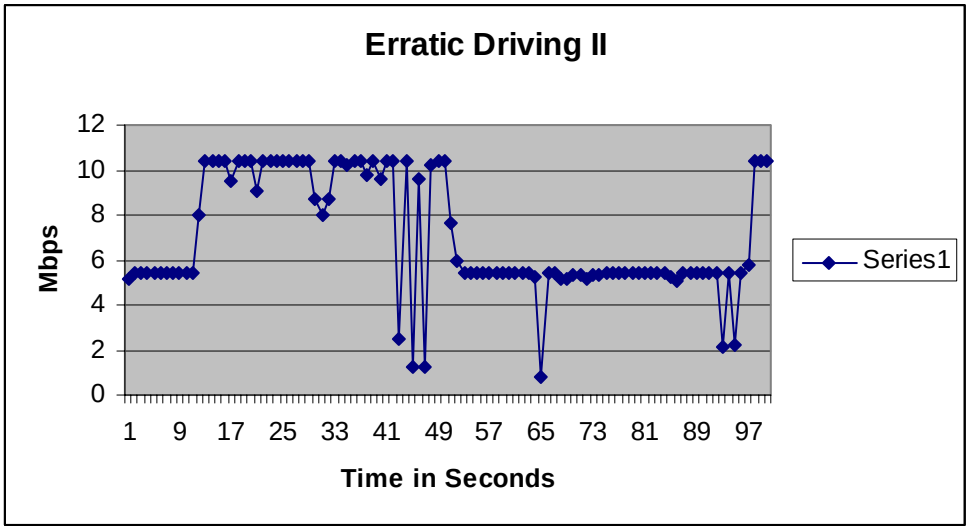

Table 3. Point Sur Erratic Driving IX Chariot results - reduced throughput due to vehicle superstructure

6. Pre-Deployment Exercises (February 2006)

Prior to deploying the COASTS 2006 network topology to Thailand, a full-scale integrated test was conducted at Fort Hunter-Liggett (FHL), CA, to test the operational capabilities of the architecture. This scenario utilized NEMESIS; a twenty-four foot long recreational vehicle (RV) converted into a multi-mission network and communications research vehicle for NPS. NEMESIS represented the deployable Tactical Operations Center (TOC) which would be established at Mae Ngat Dam in Chiang Mai, Thailand. This represented the first full establishment of the tactical network topology of the COASTS project, to include the maritime topology tested in this thesis.

The maritime network topology was evaluated in the following land-based configuration. The Redline AN-50e PtMP radio in the NEMESIS RV was connected to a 30 degree 5.8 GHz, 14-dbi antenna. The Redline AN-50M was placed in the cab of a NPS government Ford F-150 pick-up truck, and then connected to another 30 degree antenna, identical to the one on the NEMESIS RV. The antenna, placed on a six foot tripod in the bed of the pick-up truck, simulated the raised antennas to be used on the small boats in Thailand. Two COASTS team-members braced the antenna mount and turned the antenna pole to ensure the 30 degree antenna in the truck was always directed towards the antenna on the NEMESIS RV.

Figure 50. 90 Degree 5.8 GHz antenna w/ T-58 Transceiver

The FHL runway, which measured one-mile in length, was used to simulate the over-water area of operations planned for the Mae Ngat Dam exercise. Also, these tests were conducted in order to have data to support an over-land and over-water comparison.

Various driving patterns were designed for the pick-up truck in order to mirror the interdiction maneuvers of small boats in riverine and littoral maritime environs. The first driving pattern was a simple straightaway pattern conducted in order to ascertain the maximum effective distance for the given antenna configurations. The IX Chariot throughput from this iteration resulted in an average of 32 Mbps throughout the straightaway driving test.

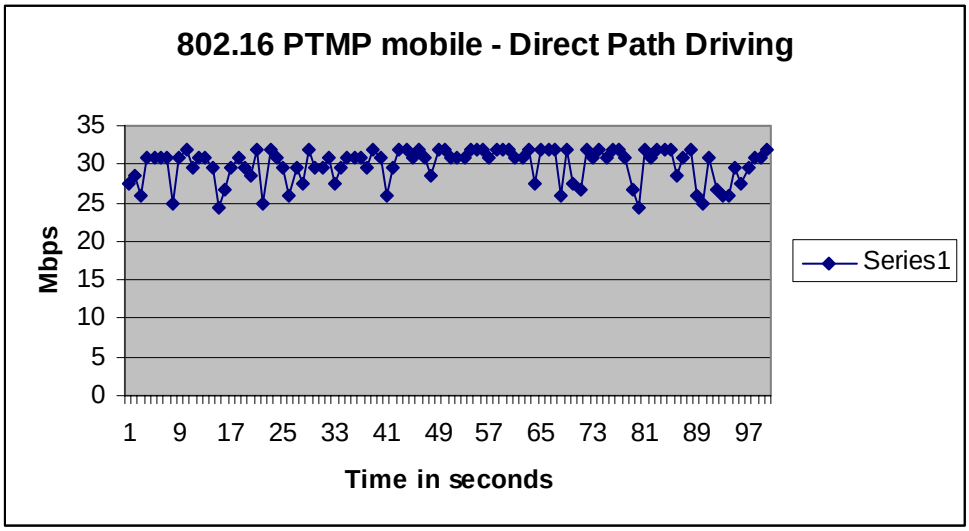

Table 4. FHL Throughput tests

The test was conducted driving away from the NEMESIS antenna, and then on the return along the runway to the RV. The data showed no degradation at a distance of over one mile over ground[137]. The terrain at the end of the runway was impassible, making it impossible to evaluate the network at greater ranges.

The repetition of the erratic driving portions from Pt. Sur, even at the greater distances of one mile from the NEMESIS RV, resulted in a throughput level comparable to the straightaway tests. An average of 32 Mbps was recorded during the usage of the rotating simulated ESA antenna despite the speeds applied to these trials[138].

[137] The measurements on this distance are ground miles (1760 yards) – later measurements will be in nautical miles during the over-water tests in Monterey, CA

[138] During the zig-zag patterns driven at speeds of 35 to 40 miles per hour (MPH)

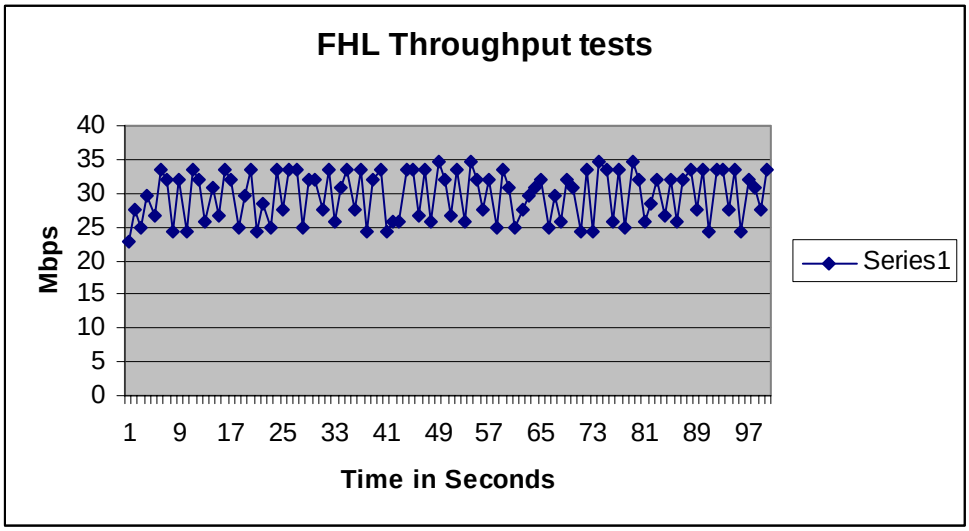

Table 5. FHL Throughput tests

During the FHL tests, service-members and civilians from the Joint Information Operations Center (JIOC) were on-hand for passive and active signal collection to prepare for Red Team scenarios to be conducted during the May Thailand deployment.

The JIOC team attempted to use RF jamming[139] in order to interfere with the IEEE 802.16 signal being used during the experiment at various stepped levels of dB. An AXIS 213 IP camera was used to conduct a visual feed alongside the IX chariot results. Also, the C3Trak chat function was used to measure the ability to maintain a data throughput alongside the video feeds and IX Chariot readouts. This way, a measured degradation could be seen in the applications on the network as well as the network itself.

The JIOC induced jamming was able to completely disrupt the camera feed from the IP camera. The moment the jamming began, the camera feed would halt. There was also a noticeable degradation in signal (observable on the IX chariot console) in the initial moments of the jamming. However, this degradation was never more than 2-4 Mbps, and the link was never degraded enough to be considered non-functional. All chat data transfer continued through the jamming.

[139] The jamming applied by the JIOC team was a layer 1 barrage jam, using superior power to disrupt the signal. There was no specific address information used to target the base station specifically. The jam was entirely centered in the Physical Layer.

Furthermore, the loss of the camera feeds created obvious indications of jamming which could be detected by an operator. The link degradation in throughput was modeled by IX Chariot below.

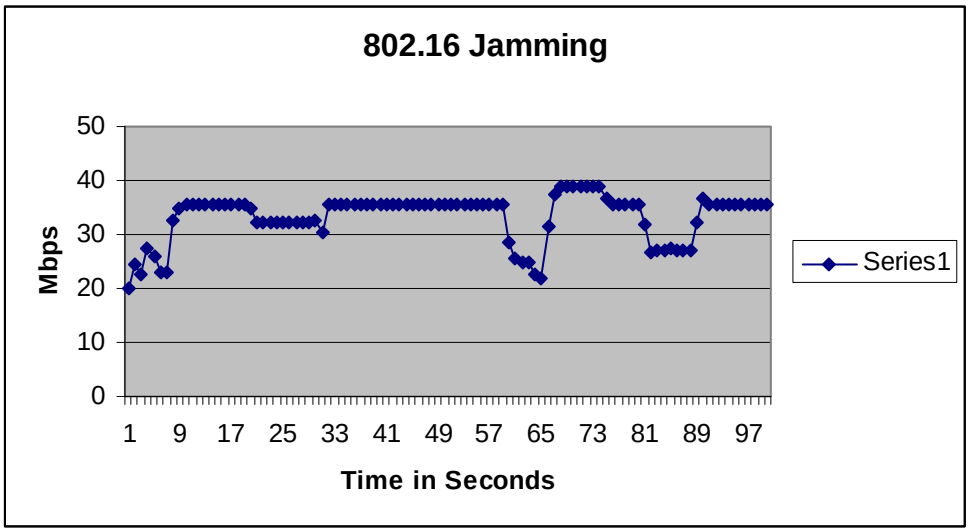

Table 6. FHL Throughput tests during JIOC Jamming

In the graph above, the short drops in Mbps can be explained by the jamming techniques. The drops to 20 Mbps occurred during periods when the JIOC team increased dB power from their RF jamming antenna. These drops to 20 Mbps were at the most significant levels attained by the antenna configuration used by JIOC during these tests.

Interestngly, the IEEE 802.16 network was fairly resistant to the jamming efforts undertaken by the JIOC Red Team at FHL. Also, the jamming attacks were easily detected by watch-standers at the TOC in the NEMESIS RV..

7. COASTS Deployment to Thailand (March 2006)

Ten students, two naval reservists, three NPS faculty, and four civilian contractors deployed to Thailand on the 20th of March, 2006. The mission goal was to establish the COASTS 2006 network topology at the Mae Ngat Dam in the Chiang Mai district of Northern Thailand. The objective of the March deployment was to test the total network architecture and rehearse the scenario for the May 2006 demonstration.

Due to various hardware and software problems with the network configuration, very little testing with the Maritime FLAK was accomplished. New design configurations for the FLAK were devised through hands-on contractor interaction.

The shore-side antennas were set up with a single two-way splitter between the T-58e Transceiver and the two Hyperlink 17 dBi antennas. A standard RJ6 cable connected the T-58e to the AN-50e[140], which was directly connected to the TOC's Tactical Communications Kit (TCK) by a CAT-6 crossover cable. The TCK, at this point, replaced the entire networking topology configuration used within the NEMESIS van during the pre-deployment tests.

Figure 51. Tactical Operating Center

From the network TOC, the various COASTS links to the operational and global strategic databases and watch stations were maintained. From the TCK (located in the bottom right of the picture), these feeds were linked and routed, and then connected to the maritime AN-50e through a 300 foot RG-6 coaxial cable line. The AN-50e was then connected to the shore arrays.

[140] The AN-50e used in the Thailand tests was configured without the increased Mbps firmware loaded on the AN-50e used during the FHL and Pt Sur PtMP tests. This was a decision made due to budget constraints, but since the RF propagation has been tested to be the same in both levels of throughput, it was considered to be a minor inconvenience. This means that the lesser bandwidth experienced in the following iterations was accounted for, and not necessarily due to any factors in the testing.

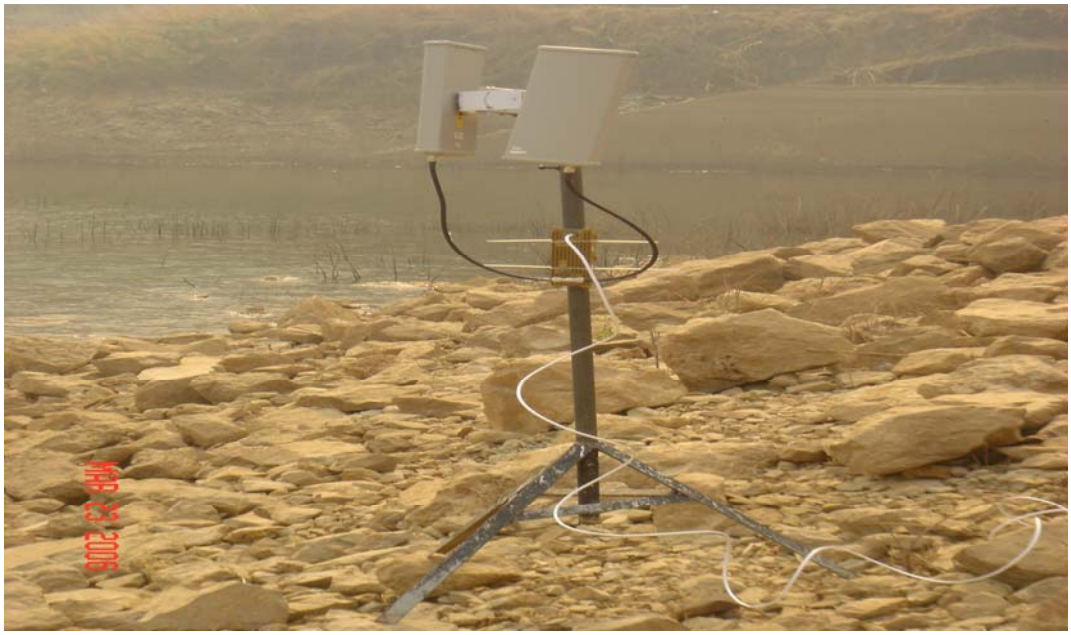

Figure 52. 180 degree array used at the Mae Ngat Dam during testing

Various different antenna configurations were used on the speed boat during testing. The first design was an array of four *Superpass* 13 dBi, 90 degree sector antennas, which were linked by RF cables, combined to a single four-way splitter. The splitter, much like the two-way splitter used on the shore array, was then connected to a T-58e by separate RF cables. The RJ6 cable then linked the T-58e to the AN-50M radio.

Figure 53. 360 degree omni-sector array using 13 dBi 90 degree sectored antennas

The Modular PC was mounted onto the SKB cases. The ability to use the Modular PC as a stationary portion of the FLAK on the boat, as well as a detached wearable module among the boarding party, makes the data-collection potential of the VBSS boarding team significantly greater than currently in use today. Upon the installation of the roto-shock SKB case to the motorboat, it was found that the form factor of the SKB case was a significant impedance to personnel movement within the boat. At this point, the intention of reducing the size of SKB case used was decided.

Figure 54. SKB Case with the Modular PC mount

The overall results of these maritime tests were less impressive than the performances in FHL only one month before. This was primarily due to the usage of four 90 degree antennas in a 360 degree array format, resulting in a reduction in RF transmission power, i.e. power was split between each of the four array antennas. As opposed to a one mile plus distance, which was observed at FHL, a distance of only three tenths of a mile could be maintained over water. Although a full 15 Mbps was achieved while the connection was maintained, the distances observed during FHL were not repeatable. After a mere half kilometer of separation, the maritime link was lost.

After some troubleshooting, the another reason for the lack of propagation was found to be due to a lack of proper antenna placement. The vertical beam width of the 90 degree sector antennas was very narrow, thus the shore and maritime antennas had to be at almost the exact same elevation.

8. Monterey USCG Maritime Tests (April 2006)

One month after the return from the March 2006 tests in Thailand, more maritime testing was conducted on the 28th of April. The USCG station Monterey was used as the shore staging area, and the USCG patrol vessel, Motor Life Boat (MLB) 47 was used as the maritime node. The lessons of the March deployment to Thailand were applied and the placement of the shore arrays was optimized based on the physical location of the maritime antenna.

A shore array was constructed using three of the Hyperlink 17dBi antennas, forming 270 degree coverage over the bay. The three antennas were linked to a T-58e transceiver by a splitter. LT Bill Wren, JP Pierson, and LT Jonathon Powers operated the shore array during the testing. LT Hochstedler embarked on MLB 47 with the reduced M-FLAK.

Figure 55. Shore Array used during PtMP testing at the USCG pier in Monterey, CA

The mobile unit, an AN-50M, was connected to a single omni-directional 12dbi antenna. A T-58e was used in the link, but no splitter was added in order to reduce the RF losses experienced in Thailand.

Both the Redline RF analyzer and an IX Chariot network analysis software suite were used to test the network links. Repeated tests of RF monitor and IX Chariot were used to check the dB levels and throughput of the signal. Incremental distance increases of 500 yards were applied during successive trials.

The resulting RF monitor feeds showed only minor degradations as the distance increased, reducing from an average of 57dB signal strength to an average of 87 dB over a period of 70 minutes[141] which correlated to a maximum effective distance of 3NM.

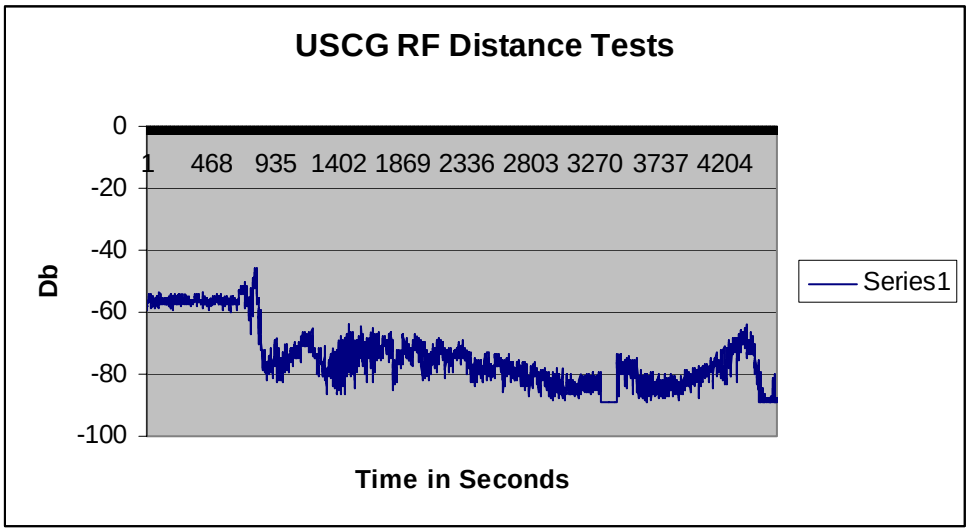

Table 7. RF distance test to 3NM in the Monterey Bay

9. COASTS Deployment to Thailand (May 2006)

Six of the students from the March deployment, along with ten naval reserve support officers and enlisted, three NPS faculty, and fifteen civilian contractors deployed for the COASTS 2006 final technology demonstration. This iteration would entail the final scenario, including the fully intended network M-FLAK periphery technologies.

New adaptations to the FLAK were implemented based on lessons learned from the March deployment, as well as ship to shore tests with the USCG on April 28th. The flowing equipment was added to the FLAK:

- SP8L Sensor Probe Eight Linux
- Patrolcam
- Kestrel USB Camera with a USB connection
- Mesh Dynamics 802.11g 400mw radio access point
- Biometric capable PDA
- VoIP Phone

[141] 89 db is where the signal is considered degraded enough to be lost.

The SKB roto-shock cases used in the first tests were replaced with an SKB roll shock case. The roto-shock case, although more than adequate, was slightly too large for use with small boats. Since the M-FLAK needs to fit on small watercraft like the longboats used on rivers in Southeast Asia, a reduced footprint from the new SKB case was required.

Upon arrival in Thailand, a new dual shore array network was constructed with two arrays established at separate locations on the dam shoreline. These two arrays were strategically placed in order to maximize the performance of the IEEE 802.16 links between the two mobile small boats, and to ultimately extend the RF range recorded during the March tests.

During the initial tests on the M-FLAK, a steady camera feed from the Patrolcam was used as a visual guideline to augment the IX Chariot and RF monitor data being received and recorded.

On May 23rd, the first M-FLAK was constructed and placed on the speedboat for testing. The first network trial involved one boat operating within the coverage area of the combined shore arrays. Initial trials mirrored the RF performance which occurred in March, where the link maintained 15Mbps, but was unable to maintain link at distances greater than one KM without losing RF connectivity. After some trouble-shooting, the configuration on the shore antennas was found to be out of alignment.

On May 24th, the M-FLAK was re-deployed with the shore antenna moved to an elevation almost ten feet higher on the dam face. Upon initialization of the link, the throughput leapt to 15Mbps again. This link was then maintained across the entire dam waterway, with NLOS connectivity maintained around the bend of the river (almost one tenth of a mile) at the same levels of throughput.

After ascertaining the network coverage for the river scenario, the speedboat was used to establish the ability of the link to be maintained by the M-FLAK at higher speeds. For the next series of trials, the speed of the boat was increased to 25 knots, the intended level of velocity to be used during the interdiction portion of the scenario. The link maintained an average throughput of 15 Mbps, although the higher speed did result in a small reduction in dB as observed on RF monitor. However small antenna alignments corrected the decreases experienced in March.

On May 25th, the same tests as conducted on May 23rd and 24th were repeated in order to show a consistent performance, as well as practice for the scenario. As the speedboat traveled across the water at a speed of 23 knots, RF monitor was used to test the dB strength of the IEEE 802.16 signal and the ability of the network to maintain connectivity. At a continual ping, only ten out of three hundred packets were dropped. Also, the RF signal never dipped during the high speed run and an increase of dB occurred at the end of the run when the range to the antenna was significantly reduced.

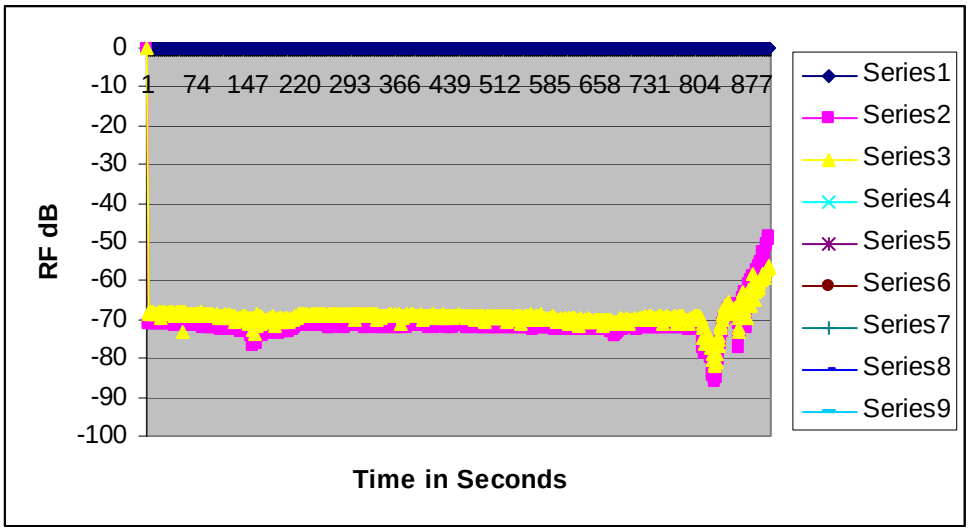

Table 8. RF Monitor Results from a high speed run (23 Knots) on the Mae Ngat Dam

Two boat tests were also conducted at the Mae Ngat Dam, with separate AN-50e's feeding dedicated T-58e transceivers and antennas on the shore antenna array. Each boat operated an M-FLAK, and was equipped with a 90 degree sector antenna. The AN-50e's operated PtP firmware, limiting the exchange between communications sectors. The results of each RF monitor and IX chariot tests mirrored the individual boat trials.

In these tests, the second M-FLAK was operated on an indigenous Thailand longboat, establishing the functionality of operating a unit on a "junk force" coalition craft.

Figure 56. LT Hochstedler operating M-FLAK on Thailand longboat

The integration of the MeshDynamic IEEE 802.11 wireless access point was the next obstacle to the completion of the M-FLAK. The M-FLAK was not able to integrate the MeshDynamic capability due to hardware issues with the network connections to the IEEE 802.16 AN-50M in the M-FLAK. However, a D-Link access point was purchased and was added to replace the MeshDynamic box. With a few hours of configuration, the addition of the D-Link box established a connection from the Modular PC to the TOC via a wireless connection. This new link enabled the Kestrel camera feed from the individual boarding officer to be transmitted back to any location on the link.

The Kestrel camera, despite being a propriety camera much like the Patrolcam, was successfully integrated on the wireless network. The video feed from the boarding camera, mounted on the shoulder of LT Hochstedler, was able to collect and transmit a consistent video and data feed through the M-FLAK IEEE 802.16 link, and to the TOC over a half mile away. With the ranges observed through field testing of the IEEE 802.16 AN-50s VBSS, harbor security, and maritime defense missions can be potentially enabled with minimal cost.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. RESEARCH SUMMARY

Equipment conforming to the IEEE 802.16 standard can fulfill the multiple C4ISR operational requirements of not only US maritime and riverine forces, but coalition assets as well. Furthermore, these technologies are COTS, and thus can be implemented in a much shorter time-frame than equipment procured through the DoD acquisition system. All of the periphery technologies tested with the M-FLAK were a success once final architectural designs were completed. Due to the high levels of mission requirements being levied on current US and coalition military forces in the GWOT, a short-term solution is not only necessary, but vital.

The NECC's riverine squadron will be deploying to Iraq in less than a year, while the US Naval Coastal Warfare forces will be deploying globally in the same time frame. These small boats need to be integrated into the current NCW mission topologies in order to enable the National Fleet concepts being directed through the QDR by the DHLS and DoD.

Concerning the end system technology which was used on the M-FLAK, there are specific requirements which need to be implemented in order to design operable equipment on the network. The strategy for the implementation of a GIG requires:

- LAN
- Terrestrial WAN
- Radio-WAN
- End-to-end security measures
- End-to-end management
- Next generation protocols

LAN – A local area network (LAN) simply needs to be architected along the lines defined previously, where all end systems should be linked to a local area network. This is emphasized in principle #1 and was done by instantiating the network along this architectural design on each small boat.

Terrestrial WAN – All LANs should be interoperable by connecting them, via a router, to a larger wide area network. The GIG-BE is defined along these lines, and will fulfill these requirements if used in this manner. No other adaptation is required due to the implemented commercial technology upon which the GIG was built. The TCK router served as the link back to the fixed internet, connecting the link via the second principle in the architecture requirements.

Radio-WAN – in order to extend the reach to mobile platforms, digital radio systems to extend the last mile reach of the network footprint to the disadvantage user are necessary. Commercial technology has only recently achieved the level of accomplishing this feat through the IEEE standards established at the turn of the century. The IEEE 802.16 standard enables the connectivity between principles #1 and #2 in the requirements addressed through the Buddenberg MANET articles.

End-to-end security measures – the passage of data across the entire information system, to include the fixed internet, regardless of its level of trustworthiness. The data must be secure from writer to user or in another manner of thought, from sensor to shooter.

Since traditional encryption is operated at layer one of the OSI model, it is susceptible to future “Walker Case” thefts. A Layer 7 end-to-end security protocol would protect the network more robustly, and with less of a footprint, than separate cryptology applications.

Protection from insider attacks needs to addressed by network security managers. All end systems must be protected at the level of security established with the rest of the network topology.

End-to-end management – the entire network must be maintained and managed. The Navy has created the necessary skill-sets with its creation of the Information Professional (IP) Officers and the merging of the traditional Radioman and Data Professional rates into the Information Tech enlisted rate. These naval personnel can easily extend their mission to incoporate commercial network technology.

Next generation protocols – Current network protocols include IPv4, TCP, OSPF, and BGP. Future protocols applicable to the military networks are: IPv6 and Nak-only reliable multicast (NORM). These protocols can greatly enhance the capabilities of current COTS technology architectures[142].

Requirements for an effective modularized MANET end system will include:

- A LAN interface
- An enveloping definition (MIME or XML are good examples)
- A means for authentication and encrypting data (e.g. S/MIME, XML-sign and –crypt)
- Setting of DSCP on exiting datagrams for QoS puposes
- An SNMP agent that affords both local and remote manageability[143]

Coalition allies are facing asymmetric threats in their waters on a regular basis. Furthermore, the need for Global ISR extends far beyond the capabilities of current US maritime platforms to reach every un-patrolled region in the world's waterways. Coalition maritime security initiatives are growing, increasing the need for interoperable networked communications capabilities.

In many cases, allies seeking to implement this technology in their maritime forces do not have the significant operating budgets to purchase extremely expensive C4ISR technology from the US. The cost of the COTS components used to build the M-FLAK averages $25,000 dollars US[144]. This per node figure does not include the cost of establishing a TOC in order to coordinate the communications links to the deployed M-FLAKs. Situational awareness applications, security applications, and satellite links are also excluded from this cost, and are considered to be applications derived from integration into the overall NCW topologies.

The characterization of political-military relations between various countries and the US establish many obstacles which prevent the large-scale deployments of US

[142] It is important to note that these protocols are not vital, and are simply noted in this thesis to highlight the future developments which can be used to enhance the current architecture without starting from the zero-point in future designs.

[143] Buddenberg, "Objective, Architecture, and Strategy for Network-Centric: A Perspective on Mobile Communications, pg. 3

[144] These figures include no calculations concerning maintenance, up-keep, and life-cycle costs. This is simply an analysis of equipment purchase. Any assessment of total cost must integrate the total architecture, long-term acquisition costs, and spiral upgrades through the full life-cycle of the system.

military forces into other countries' territories. A reduced presence which revolves around a limited personnel footprint, but a significant amount of support in the form of intelligence collection and increased NCW capabilities needs to be implemented. In the maritime theatres of rivers and littoral waters, these situations are perhaps the most difficult locations to extend "last mile" reach. By implementing the M-FLAK into these locations, the future of maritime security and riverine operations will be connected into the future of NCW in the GWOT.

B. LESSONS LEARNED

The M-FLAK performs successfully in adverse environments, to include the severe riverine domain of the Mekong River tributaries in Thailand. Consistent temperature and humidity measurements were taken throughout the testing in Thailand and California by the COASTS Data Collection team, and there was no reduction in RF connectivity or throughput during periods of extreme heat and rainfall[145]. Significant bandwidth was maintained at all speed profiles, to include interdiction speeds. RF connectivity was maintained over a significant distance in the majority of the tests and trials.

The main obstacle to establishing a small boat IEEE 802.16 network topology is the initial antenna configuration. Once the antenna configuration was established, the follow-on configuration changes were simple and easy to implement. The next significant obstacle was the difficulty of dealing with and integrating proprietary technologies.

It is important to note that these assessments in the lessons learned section concern the current COTS technologies. Newer technologies will always be developed as end systems, and the ability to upgrade to these newer systems must be apart of any acquired network architecture. Therefore these lessons learned are merely observations concerning the current M-FLAK end systems used.

[145] Antenna configuration accounted for the reduced distanced experienced during the March 2006 Tests in Thailand. Topography resulted in the reduced distances experienced in the December 2005 tests at Pt Sur, CA.

1. Overall Network Lessons Learned

a. IEEE 802.16 Antenna Placement

The most important lesson for the network topology is the proper analysis of RF study prior to antenna placement. The amount of time spent adjusting antennas, calculating Fresnel zone limits, and changing out antennas severely interfered with the time available for research. Usage of RF analyzers to test the propagation in the region will also greatly reduce the set-up time needed to establish these networks in the field.

b. AN-50e and AN-50M Terminals

The COASTS field experiments resulted in continual losses of AN-50s, both E and M, through operator error. The AN-50's IF ports can be damaged to the point of inoperability by simply not tightening the connections on the RJ6 cables when the unit is turned on. This delicate portion of the radio system requires adjustment in order to prevent continual losses of equipment during operational missions.

2. End Systems Technologies

a. Kestrel Camera

The Kestrel camera performed as required, transmitting feeds through the network. Continued research into fully integrating the camera as an IP camera is recommended. As an IP camera, necessary software applications were required to utilize it during boarding operations and were added separately from the hardware. Adding a firmware IP protocol would be expensive, but it would simplify the ability to include the video feed into current and future SSAs.

Per the end system "good citizen" requirements, the Kestrel camera, in its current incarnation, is not adequate for the defined architecture. It required a software application to possess a LAN interface, which established its lack of the other parameters. Changing the Kestrel to be a LAN camera with the rest of the end system architecture requirements will greatly enhance a wonderful proprietary technology to a full network camera.

b. Patrolcam

The Patrolcam performed extremely well in the maritime environment. The video feeds were clear and easy to manipulate.. The steer-able capability of the camera enabled a target of interest to be tracked at great distances[146]. The Patrolcam had to be hard-mounted into place in order to receive the best video feeds from the camera. When the camera was first placed into position, it jittered from the vibration of the speedboat engine.

Also, since the Patrolcam is a proprietary technology, it does not feed directly into the SSA. Much like the Kestrel unit, a firmware addition which would include the camera on a TCP/IP protocol, would greatly expand the versatility of the package.

Furthermore, the Patrolcam cannot function without technologies to make it LAN-interface capable. This also means that there are no conflicting software applications which need to be removed in order to develop the Patrolcam into a fully developed networked end system.

c. Identix IBIS

The Identix biometric device performed well in the field. Fingerprints and photographs were easily taken by the device. Integration of the handheld unit applications into the Modular PC and the Kestrel camera would greatly reduce the footprint of the M-FLAK equipment.

The IBIS is a TCP/IP product, and therefore can be a fully configured and networked end system. With the LAN interface, biometric data can be passed from the unit to any receiving server on the network. Due to the inability to fully the integrate the IBIS on this deployment to Thailand, the rest of the network capabilities were unable to be tested.

There was considerable effort placed into establishing the Identix biometrics server onto the COASTS network. This was due to the short timeframe

[146] Over one mile in range

between the receipt of the device, and the final deployment to Thailand for the scenario. Since the technology is TCP/IP based, network configuration simply requires lead-time and proper network management.

d. Modular PC

The addition of the Modular PC to the M-FLAK enabled the ease of personal computing in the extreme adverse conditions of Northern Thailand. With an average of 100 degrees Fahrenheit during mid-day testing, and a near continual rainfall in the May scenarios, the Modular PC operated with 100 percent success in the field.

The Modular PC will expand its ability to function in military applications through MIL-STD hardening of the wearable module. Also, there are integrated keyboards which dual as screen shields for the module and are being developed for future design iterations of this unique computer design.

The Modular PC is capable to be a totally networked end system. With the fully functional operating system, the modular unit can handle any software loads to improve the secondary parameters to support the LAN interface with the network.

C. FUTURE RESEARCH AREAS AND QUESTIONS

There are a myriad of directions which can be taken in continued research on the M-FLAK. The primary ones will focus on the network design according to the two MANET principles of NCW. The secondary ones will focus on the refinements concerning end system technologies, primarily in the focus of creating more network "good citizens" for a more developed MANET architecture.

1. Critical Research Areas

a. Electronic Steerable Antennas (ESA)

Although omni-directional and array antennas were the primary means of RF propagation used in this research, alternate tests were conducted with various simulated steerable antennas. Further research into the development of an electronic-steerable antenna could greatly increase the versatility of the maritime FLAK.

At Fort Hunter-Liggett, a single 30 degree antenna was used on the "shore" station and on the simulated small boat. Even when driving at speeds of 40 mph in a zig-zag pattern, close to 32 Mbps was maintained - at a range of over one mile. Although similar results were achieved during tests in Monterey with an omni-directional antenna, the ability to connect over greater and greater ranges could be achieved by using multiple ESA antenna connections.

Furthermore, an IP camera link was maintained throughout testing, with video being passed over the PtMP network at a close to real-time speed. Building on this foundation, ESA style antennas would be ideal for the mobile applications involving high speed vessels.

b. IEEE 802.16 Amplifiers

The use of amplifiers in conjunction with an IEEE 802.16 network topology has not been studied in depth relative to military applications. According to the manufacturer, reductions in bandwidth will result when amplifying the current Redline AN-50 signal, and ultimately a significant loss of data throughput. This throughput may cause losses much like RF interference in IEEE 802.16, where OFDM enables enough data to pass in order to maintain PtP and PtMP data links. In situations where range in NLOS environments would be necessary as opposed to wider bandwidth, this capability could be expanded by the use of amplifiers.

Also the management of amplifiers in the post-splitter position on the shore and ship based antenna arrays is a recommended area of research.

c. Norsat 5200 KU-10W-P3K

The Norsat Corporation has added a new satellite communications kit to its inventory which would complement the maritime FLAK, particularly in the remote riverine environment. The NORSAT fulfills the satellite mobility link to the M-FLAK by linking a TC/ICP network at an uplink/downlink speed of over 4Mbps.

Some riverine missions will entail a total separation from other GCE and composite forces for recon, and a connection along a land-based network topology will not be available. A portable satellite connection would be ideal in these long-range OTH missions.

d. Riverine Maritime Security Coalition Communications Doctrine

The adaptation of coalition communications into so many aspects of the maritime security and riverine requires a further expansion of the writings on these subjects. Every interaction with the Thai military highlighted lessons learned which needed to be incorporated into testing parameters. This issue is extremely important for countries not restricted by FCC regulations. For example, the Royal Thai Air Force employed a 5W 802.11g air-to-ground network link which had adverse effects upon the COASTS network performance. Since riverine warfare has shown a consistent requirement for joint operations, to include Close Air Support (CAS), the network configurations of deployed collation forces will continue to be a source of concern.

e. Alternate COTS IEEE 802.16 Commercial Vendors

When this thesis was initially launched, Redline Communications was the only vendor of commercial IEEE 802.16 equipment. They also produced the only mobile IEEE 802.16 unit. Since then, new companies have produced IEEE 802.16 technology with different technological capabilities which should be tested in comparison with Redline Communications equipment. For example, Orthogon Systems, Inc. has produced a networking suite which incorporates new advances in mobile IEEE 802.16 technologies:

- I-OFDM – Intelligent Orthogonal Frequency Division Multiplexing
- Multi-Beam / Space Time Coding
- Advanced Spectrum Management with Intelligent Dynamic Frequency Selection
- Inherent Spatial Diversity
- Adaptive Modulation[147]

[147] Orthogon Technologies, pg. - 2 November 2, 2005

According to Orthogon press releases, these adaptations to the IEEE 802.16 standard achieve 99.99% reliability at service levels as high as 300 Mbps at ranges of 20 miles over water[148]. These capabilities should be tested in comparable situations as the Redline equipment.

f. Multi-boat PtMP IEEE 802.16 Testing

The time restraints on the research project resulted in insufficient time to conduct multi-boat testing with a PtMP array. All multi-boat testing was conducted using multiple AN-50s and feeding individual T-58es and antennas. A worthwhile addition to M-FLAK testing would be an examination of multi-boat throughput testing, as well as RF monitoring for the range of the signals.

By managing PtMP antennas, more versatile and cost-effective maritime security topologies could be implemented. It will be easier to connect multiple, moving small boats, with a PtMP antenna design and firmware upload than with multiple single PtP arrays. Also, multiple boat testing between a PtMP array and PtP array would establish the parameters between the two topologies.

g. Alternate Network Topologies

Fortress Technologies, Inc. is developing a mobile networking suite, which combines WAN and LAN technologies in a single encrypted box. The device, if it performs at comparable levels to the combined Redline Communications and Mesh Dynamics, equipment would greatly reduce the logistics behind the M-FLAK. It would also reduce costs by integrating the total Fortress Technologies encrypted suite into the technology.

2. Secondary Research Areas

a. Riverine M-FLAK CONOPS

A Concept of Operations for integrating the M-FLAK into NECC operations will be needed. The tactical decisions made concerning the capabilities of small boats outfitted with the M-FLAK needs to be analyzed in the various missions they

[148] Ibid

will undertake. Specific doctrines for VBSS and maritime security missions need to be analyzed, as well as the multiple objectives established for future USN riverine forces.

The training of small boat operators should also be studied in the M-FLAK CONOPS.

b. Extended M-FLAK Periphery Technologies

The shortage of research time and funding resulted in some peripheral tests not being completed. An integration of VOIP communication, sensor suites, and newer biometrics gear could be advanced. The more technology that can be integrated into the Modular PC the more benefit from a logistics stand-point. The IBIS could be easily integrated into the computerized functions of the modular PC. Also, software packages could be implemented to remove the need for a separate VoIP phone.

c. Design of a USCG Coastal Maritime Radio-WAN

With the USCG's UHF-FM analog communications infrastructure already in place around the country, an accurate cost/time analysis of the placement of IEEE 802.16 Radio-WAN architecture, linked into a fixed GIG connection, could be produced. With a thorough study of geography and topography, in combination with RF analysis, a reasonable link budget could be designed for the optimum placement of antennas and equipment in order to fully cover the maritime domain.

3. Tertiary Research Areas

a. Integration into the Hastily Formed Network (HFN) Humanitarian Assistance/Direct Response (HA/DR)

After the success of the NPS HFN project following the 2005 tsunami in Thailand and the Hurricane Katrina response to New Orleans in the same year, the advantages of integrating similar joint and coalition wireless communications capabilities became apparent. Currently, the NPS HFN project is conducting Ship to Operational Maneuver (STOM) research off the coast of Indonesia with the USNS Mercy. The integration of the M-FLAK into these testing parameters would be a significant extension of the National Fleets' ability to contribute to HA/DR missions.

b. Life-cycle Management Costs of Operating a Squadron of Small Boats with the M-FLAK

The full costs of designing, managing, and operating a small boat squadron operating with an M-FLAK topology in various scenarios, i.e. VBSS, riverine warfare, and harbor security, would be beneficial to the implementation for the system in the long-term. Since various small boat forces have different mission requirements, there are numerous financial management, training, and operational variables which can be analyzed.

D. SUMMARY

Overall, the performance of the IEEE 802.16 network topology was equal to the mission requirements of creating a modular C4ISR FLAK to counter threats in the asymmetric maritime theatre. Based on the current threats to US and coalition assets in the maritime theatre, a NCW command and control capability needs to be introduced in to the various small boat maritime forces around the globe. The sooner the US extends into IEEE 802.16 technologies in a formalized program in order to enhance our real-time NCW capabilities at the tactical level, the sooner the maritime forces, in their multiple mission areas, can meet these threats.

LIST OF REFERENCES

Caceres, Francisco, and Swearingen, Brad "Analysis of the 802.11b and IEEE 802.16 Technologies as a part of the Tactical Internet." Naval Postgraduate School (NPS). Monterey, CA. September 2005.

Clark, Vern ADM. "Projecting Decisive Joint Capabilities – Sea Power 21 Series Part I." Proceedings. Naval Institute. Annaplois, MD. October 2002.

Buddenburg, Rex. "Of Good Network Citizens and Network Toasters." Naval Postgraduate School (NPS). Monterey, CA. September 1997. Version 2 published February 2000.

Buddenburg, Rex. "Objective, Architecture and Strategy for Network-Centric: A Perspective on Mobile Communications" Naval Postgraduate School (NPS). Monterey, CA. September 2002.

Comer, Douglas E. Computer Networks and Internets with Internet Applications. Pearson Education Inc. Upper Saddle River, NJ. 2004.

Cutler, Thomas J. Brown Water, Black Berets: Coastal and Riverine Warfare in Vietnam. Bluejacket Books. Naval Institute Press. Annapolis, MD. 1988.

Dunnavent, R Blake. Brown-Water Warfare: The US Navy in Riverine Warfare and the Emergence of a Tactical Doctrine, 1775-1970. University Press of Florida. Tallahassee, FL. 2003.

Guice, Robert J., and Munoz, Ramon J. "IEEE 802.16 Commercial off the Shelf (COTS) Technologies as a Complement to Objective Maneuver (STOM) Communications." Naval Postgraduate School (NPS). Monterey, CA. September 2004.

Klopson, Jadon E. and Burdian, Stephen V. "Collaborative Applications used in a Wireless Environment at Sea for use in Coast Guard Law Enforcement and Homeland Security Missions." Naval Postgraduate School (NPS). Monterey, CA. March 2005.

Lancaster, Dwayne "Developing a Fly-Away Kit (FLAK) to Support Hastily Formed Networks (HFN) for Humanitarian Assistance and Disaster Relief (HA/DR). Naval Postgraduate School (NPS). Monterey, CA. June 2006.

Martoglio, Charles, and Morgan, John Jr. "Global Maritime Network." Proceedings. Naval Institute Press. November 30, 2005.

Mills, Eric "An Integrated Battle Space: Riverine Warfare Conference Final Wrap-up." Naval Institute Seminar. Annapolis, Md. April 6-7, 2006.

Mukundun, Pottengal CAPT. “Iraq Declared new Piracy Hotspot.” International Maritime Bureau (IMB) Piracy Reporting Center (PRC) January 31, 2005.

Rourke, Ronald O’ “CRS Report to Congress: Navy Role in the Global War on Terrorism (GWOT) – Background and Issues for Congress” Washington, D.C. February 6, 2006.

Rourke, Ronald O’. “CRS Report to Congress: Homeland Security: Coast Guard Operations – Background and Issues for Congress.” Washington, D.C. July 1, 2004.

Russell, James. “Maritime Security in the Gulf: Addressing the Terrorist Threat.” Insights Issue No 2. February 2006.

Simon, Sheldon W. “Southeast Asia: Back to the Future?” Strategic Asia: 2004-2005: Confronting Terrorism in the Pursuit of Power. National Bureau of Asian Research. Seattle, WA. 2006.

Stubbs, Bruce B. “Smarter Security for Smaller Budgets: Shaping Tomorrow’s Navy and Coast Guard Maritime Security Capabilities.” The Heritage Foundation. May 17, 2005.

Valencia, Mark J., and Young, Adam J. “Conflation of Piracy and Terrorism in Southeast Asia: Rectitude and Utility.” Contemporary Southeast Asia. Vo. 25, No 2. August 2003.

Wiley, Paul. “The Art of Riverine Warfare from an Asymmetrical Approach.” Naval Postgraduate School (NPS). Monterey, CA. March 2004.

“COASTS Concept of Operations 2006.” Naval Postgraduate School. Monterey, CA 04 January 2006.

“COASTS Operational Order – March 2006.” Naval Postgraduate School. Monterey, CA. 06 March 2006.

“COASTS Operational Order – May 2006.” Naval Postgraduate School. Monterey, CA. 20 April 2006.

Department of Defense (DoD) DoD Report to Congress: Network Centric Warfare. www.dod.mil/nii/NCW/ncw_exec_sum.pdf Downloaded on March 17th, 2006. Posted on September 2004.

“Global Information Grid (GIG) Overarching Policy” Department of Defense Directive 8100.1. Washington, D.C. September 19, 2002.

“The Implementation of Network-Centric Warfare.” Director, Force Transformation, Office of the Secretary of Defense. Department of Defense. Washington, DC. January 5, 2005.

"Joint Vision: 2020." Joint Chiefs of Staff (JCS). Department of Defense (DoD). Washington, DC. June 2000.

"Maritime Strategy for Homeland Security." United States Coast Guard (USCG). Washington D.C. December 2002.

"National Security Strategy (2002)." Washington, D.C. September 2002.

"National Strategy for Homeland Security. Washington D.C. July 2002.

"Quadrennial Defense Review Report." Washington, D.C. February 6, 2006.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Mr. James F. Ehlert
   Director, Maritime Domain Protection Research Group (MDP-RG)
   Naval Postgraduate School
   Monterey, California,

4. Colonel Thomas Lee Williams
   Deputy Science Advisor
   U.S. Pacific Command (USPACOM)
   Camp Smith, Hawaii

5. Mr. Russ Holland, Chief of Staff
   Joint Inter-Agency Task Force West (JIATF-W)
   Camp Smith, Hawaii

6. Mr. Kurt Badescher
   US Special Operations Command (USSOCOM)
   Tampa, Florida

7. Mr. J. Christopher Griffin,
   Westwood Computer Corporation
   Charlotte, North Carolina

8. Mr. Ralph L. Boyce, US Ambassador of Thailand
   US Department of State (DoS)
   Bangkok Thailand

9. Lt Col Mel Prell, USAF
   Joint US Military Advisory Group Thailand (JUSMAGTHAI)
   Bangkok Thailand

10. Lieutenant General Krita Kritakara
    Deputy Secretary
    Thailand National Security Council (NSC)
    Bangkok. Thailand

11. Lieutenant General Apichart
Director-General, Defence Research & Development Office (DRDO)
Parkred, Nonthaburi,

12. Group Captain Dr. Triroj Virojtriratana
DRDO COASTS Project Manager
Parkred, Nonthaburi,

13. Group Captain Wanchai Tosuwan
Director, Research & Development Promotion Division
Parkred, Nonthaburi,

14. Group Captain Teerachat Krajomkeaw
Directorate of Operations
Royal Thailand Air Force (RTAF) Headquarters
Bangkok, Thailand

15. Mr. John Laine
Senior Contractor, JIATF-West
Interagency Intelligence Fusion Center (IIFC)
Chang Mai, Thailand

16. Mr. Robert Sandoval
Joint Intelligence Operations Command (JIOC)
San Antonio, Texas

17. John Taylor
President, Mercury Data Systems
Greensboro, North Carolina

18. Captain Phil Erdie, USMC
U.S. Marine Corp Systems Command (MARCORSYSCOM)
Quantico, Virginia

19. Mr. Thomas Latta
C4ISR & IO PM
Space and Naval Warfare Systems Command
Norfolk, Virginia

20. RADM Nimmick, USCG
Maritime Intelligence Fusion Center (MIFC)
Alameda, California

21. Mr. Curtis White
Commander's Representative
USAF Force Protection Battle Lab
Lackland AFB, Texas

22. USCG Headquarters
Washington, DC
Att: MCPO Wright

23. Mr. Archie Newell
Cisco Systems

24. Mr. Mike Rathwell
Identix Corporation
Jersey City, New Jersey

25. Dr. Leonard Ferrari
Dean of Research
Naval Postgraduate School
Monterey, California

26. Dr. Pat Sankar
NPS Distinguished Fellow
Naval Postgraduate School
Monterey, California

27. Dr. Gurminder Singh
Director of the Center for the Study of Mobile Devices and Communications
Naval Postgraduate School
Monterey, California

28. Dr. Carlos Borges
Mathematics Department
Naval Postgraduate School
Monterey, California

29. Dr. Frank Shoup
Director of Research, Meyers Institute, GSEAS
Naval Postgraduate School
Monterey, California

30. Dr. Dan Boger
Chairman of the Graduate School of Information Sciences
Naval Postgraduate School
Monterey, California